Edizione provvisoria

SENTENZA DELLA CORTE (seduta plenaria)

30 aprile 2024 (*)

Indice

«Rinvio pregiudiziale – Trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche – Direttiva 2002/58/CE – Riservatezza nelle comunicazioni elettroniche – Tutela – Articolo 5 e articolo 15, paragrafo 1 – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 11 e articolo 52, paragrafo 1 – Normativa nazionale diretta a combattere, mediante l'azione di un'autorità pubblica, le contraffazioni commesse in Internet – Procedura della cosiddetta «risposta graduata» – Raccolta a monte, da parte di organismi degli aventi diritto, degli indirizzi IP utilizzati per attività lesive dei diritti d'autore e o dei diritti connessi – Accesso a valle, da parte dell'autorità pubblica incaricata della tutela dei diritti d'autore e dei diritti connessi, a dati relativi all'identità civile corrispondenti a detti indirizzi IP conservati dai fornitori di servizi della di comunicazioni elettroniche – Trattamento automatizzato – Necessità di un previo controllo da parte di un giudice o di un organismo amministrativo indipendente – Condizioni sostanziali e procedurali – Garanzie contro i rischi di abuso nonché contro ogni rischio di accesso a tali dati e ogni uso illeciti degli stessi»

Nella causa C-470/21,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dal Conseil d'État (Consiglio di Stato, Francia), con decisione del 5 luglio 2021, pervenuta in cancelleria il 30 luglio 2021, nel procedimento

La Quadrature du Net,

Fédération des fournisseurs d'accès à Internet associatifs,

Franciliens.net,

French Data Network

contro

Premier ministre,

Ministère de la Culture,

LA CORTE (seduta plenaria),

composta da K. Lenaerts, presidente, L. Bay Larsen, vicepresidente, A. Arabadjiev, A. Prechal (relatrice), K. Jürimäe, C. Lycourgos, E. Regan, T. von Danwitz, F. Biltgen, N. Piçarra, Z. Csehi, presidenti di sezione, M. Ilešič, J.-C. Bonichot, S. Rodin, P.G. Xuereb, L.S. Rossi, I. Jarukaitis, A. Kumin, N. Jääskinen, N. Wahl, I. Ziemele, J. Passer, D. Gratsias, M.L. Arastey Sahún e M. Gavalec, giudici,

avvocato generale: M. Szpunar

cancelliere: V. Giacobbo e M. Krausenböck, amministratrici

vista la fase scritta del procedimento e in seguito all'udienza del 5 luglio 2022,

considerate le osservazioni presentate:

– per La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net e French Data Network, da A. Fitzjean Ó Cobhthaigh, avocat;

– per il governo francese, da A. Daniel, A.-L. Desjonquères e J. Illouz, in qualità di agenti;

– per il governo danese, da J.F. Kronborg e V. Pasternak Jørgensen, in qualità di agenti;

– per il governo estone, da M. Kriisa, in qualità di agente;

– per il governo finlandese, da H. Leppo, in qualità di agente;

– per il governo svedese, da H. Shev, in qualità di agente;

– per il Regno di Norvegia, da F. Bergsjø, S.-E. Dahl, J.T. Kaasin e P. Wennerås, in qualità di agenti;

– per la Commissione europea, da S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal e F. Wilman, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 27 ottobre 2022,

vista l'ordinanza di riapertura della trattazione orale del 23 marzo 2023 e in seguito all'udienza del 15 maggio 2023,

considerate le osservazioni presentate:

– per La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net e French Data Network, da A. Fitzjean Ó Cobhthaigh, avocat;

– per il governo francese, da R. Bénard, J. Illouz e T. Stéhelin, in qualità di agenti;

– per il governo ceco, da T. Suchá e J. Vláčil, in qualità di agenti;

– per il governo danese, da J.F. Kronborg e C.A.-S. Maertens, in qualità di agenti;

– per il governo estone, da M. Kriisa, in qualità di agente;

– per l'Irlanda, da M. Browne, Chief State Solicitor, nonché da A. Joyce e D. O'Reilly, in qualità di agenti, assistiti da D. Fenelly, BL;

– per il governo spagnolo, da A. Gavela Llopis, in qualità di agente;

– per il governo cipriota, da I. Neophytou, in qualità di agente;

– per il governo lettone, da J. Davidoviča e K. Pommere, in qualità di agenti;

– per il governo dei Paesi Bassi, da E.M.M. Besselink, M.K. Bultermann e A. Hanje, in qualità di agenti;

– per il governo finlandese, da A. Laine e H. Leppo, in qualità di agenti;

– per il governo svedese, da F.-D. Göransson e H. Shev, in qualità di agenti;

– per governo norvegese, da S.-E. Dahl e P. Wennerås, in qualità di agenti;

– per la Commissione europea, da S.L. Kalėda, H. Kranenborg, P.-J. Loewenthal e F. Wilman, in qualità di agenti;

– per il Garante europeo della protezione dei dati, da V. Bernardo, C.-A. Marnier, D. Nardi e M. Pollmann, in qualità di agenti;

– per l'Agenzia dell'Unione europea per la cibersicurezza, da A. Bourka, in qualità di agente,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 28 settembre 2023,

ha pronunciato la seguente

Sentenza

1 La domanda di pronuncia pregiudiziale verte, in sostanza, sull'interpretazione della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11) (in prosieguo: la «direttiva 2002/58»), letta alla luce della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

2 La domanda è stata presentata nell'ambito di una controversia tra, da un lato, La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net e French Data Network e, dall'altro lato, il Premier ministre (Primo ministro, Francia) e il ministre de la Culture (Ministro della Cultura, Francia), in merito alla legittimità del décret n° 2010-236, du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé «Système de gestion des mesures pour la protection des œuvres sur internet» (decreto n. 2010-236, del 5 marzo 2010, relativo al trattamento automatizzato di dati personali

autorizzato dall'articolo L. 331-29 del codice della proprietà intellettuale denominato «Sistema di gestione delle misure per la protezione delle opere su Internet») (JORF n. 56 del 7 marzo 2010, testo n. 19), come modificato dal décret n° 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (decreto del 6 maggio 2017, n. 2017-924, relativo alla gestione dei diritti d'autore e dei diritti connessi da parte di un organismo di gestione di diritti e recante modifica del codice della proprietà intellettuale) (JORF n. 109 del 10 maggio 2017, testo n. 176) (in prosieguo: il «decreto n. 2010-236»).

Contesto normativo

Diritto dell'Unione

Normativa relativa alla protezione dei dati personali

– *Direttiva 95/46/CE*

3 Contenuto nella sezione II, intitolata «Principi relativi alla legittimazione del trattamento dei dati», del capo II della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31), l'articolo 7 di quest'ultima era così formulato:

«Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando:

(...)

f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1».

4 L'articolo 13, paragrafo 1, di detta direttiva disponeva quanto segue:

«Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia:

(...)

g) della protezione della persona interessata o dei diritti e delle libertà altrui».

– *RGPD*

5 L'articolo 2 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1; in prosieguo: il «RGPD»), intitolato «Ambito di applicazione materiale», ai paragrafi 1 e 2 così dispone:

«1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Il presente regolamento non si applica ai trattamenti di dati personali:

(...)

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse».

6 L'articolo 4 del RGPD, intitolato «Definizioni», precisa quanto segue:

«Ai fini del presente regolamento s'intende per:

1) "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); (...)

2) "trattamento" qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(...)».

7 L'articolo 6 del suddetto regolamento, intitolato «Liceità del trattamento», al paragrafo 1 così prevede:

«Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

(...)

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti».

8 L'articolo 9 di detto regolamento, intitolato «Trattamento di categorie particolari di dati personali», al paragrafo 2, lettere e) e f), prevede che il divieto di trattamento di taluni tipi di dati personali che rivelino, segnatamente, dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica non si applica qualora il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato o esso sia necessario, in particolare, per accertare, esercitare o difendere un diritto in sede giudiziaria.

9 L'articolo 23 del RGPD, intitolato «Limitazioni», al paragrafo 1, così dispone:

«Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

(...)

i) la tutela dell'interessato o dei diritti e delle libertà altrui;

j) l'esecuzione delle azioni civili».

Normativa relativa alla protezione dei dati personali

– *Direttiva 2002/58*

10 I considerando 2, 6, 7, 11, 22, 26 e 30 della direttiva 2002/58 sono così formulati:

«(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla [Carta]. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(...)

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(...)

(11) La presente direttiva, analogamente alla direttiva [95/46], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950], come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(...)

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati (...) può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento. (...)

(...)

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari. (...)».

11 Ai sensi dell'articolo 2 della direttiva 2002/58, intitolato «Definizioni»:

«(...)

Si applicano inoltre le seguenti definizioni:

a) “utente”: qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

b) “dati relativi al traffico”: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) “dati relativi all’ubicazione”: ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico;

(...)».

12 L’articolo 3 di tale direttiva, intitolato «Servizi interessati», prevede quanto segue:

«La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

13 Ai sensi dell’articolo 5 di tale direttiva, intitolato «Riservatezza delle comunicazioni»:

«1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l’ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell’articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.

(...)

3. Gli Stati membri assicurano che l’archiviazione di informazioni oppure l’accesso a informazioni già archiviate nell’apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l’abbonato o l’utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l’altro sugli scopi del trattamento. (...)».

14 L’articolo 6 della suddetta direttiva, intitolato «Dati sul traffico», così prevede:

«1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l’articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l’abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.

3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l’abbonato o l’utente a cui i dati si riferiscono abbia espresso preliminarmente il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

(...)

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività».

15 L'articolo 15 della direttiva 2002/58, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», è così formulato:

«1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, [TUE].

(...)

2. Le disposizioni del capo III della direttiva [95/46] relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

(...)».

– *Direttiva (UE) 2016/680*

16 L'articolo 1 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89), intitolato «Oggetto e obiettivi», al paragrafo 1 prevede quanto segue:

«La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica».

17 L'articolo 3 di detta direttiva, intitolato «Definizioni», così dispone:

«Ai fini della presente direttiva si intende per:

(...)

7. "autorità competente":

a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

(...)».

Normativa relativa alla tutela dei diritti di proprietà intellettuale

18 L'articolo 8 della direttiva n. 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale (GU 2004, L 157, pag. 45, e rettifica in GU 2004, L 195, pag. 16), intitolato «Diritto d'informazione», così dispone:

«1. Gli Stati membri assicurano che, nel contesto dei procedimenti riguardanti la violazione di un diritto di proprietà intellettuale e in risposta a una richiesta giustificata e proporzionata del richiedente, l'autorità giudiziaria competente possa ordinare che le informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale siano fornite dall'autore della violazione (...)

2. Le informazioni di cui al paragrafo 1 comprendono, ove opportuno, quanto segue:

a) nome e indirizzo dei produttori, dei fabbricanti, dei distributori, dei fornitori e degli altri precedenti detentori dei prodotti o dei servizi, nonché dei grossisti e dei dettaglianti;

(...)

3. I paragrafi 1 e 2 si applicano fatte salve le altre disposizioni [legislative e] regolamentari che:

a) accordano al titolare diritti d'informazione più ampi;

b) disciplinano l'uso in sede civile o penale delle informazioni comunicate in virtù del presente articolo;

c) disciplinano la responsabilità per abuso del diritto d'informazione;

d) accordano la possibilità di rifiutarsi di fornire informazioni che costringerebbero i soggetti di cui al paragrafo 1 ad ammettere la sua partecipazione personale o quella di parenti stretti ad una violazione di un diritto di proprietà intellettuale; oppure

e) disciplinano la protezione o la riservatezza delle fonti informative o il trattamento di dati personali».

Diritto francese

CPI

19 L'articolo L. 331-12 del codice della proprietà intellettuale, nella versione in vigore alla data della decisione contestata dalle ricorrenti nel procedimento principale (in prosieguo: il «CPI»), così dispone:

«La Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet [Alta Autorità per la diffusione delle opere e la protezione dei diritti su Internet; in prosieguo: la "Hadopi"] è un'autorità pubblica indipendente. (...)».

20 L'articolo L. 331-13 di tale codice così prevede:

«La [Hadopi] espleta:

1° Una funzione di incoraggiamento per lo sviluppo dell'offerta legale e di monitoraggio dell'uso lecito e illecito di opere e oggetti cui è collegato un diritto d'autore o un diritto connesso sulle reti di comunicazione elettronica utilizzate per la fornitura di servizi di comunicazione pubblica on-line;

2° Una funzione di protezione di tali opere e oggetti nei confronti delle violazioni di tali diritti commesse sulle reti di comunicazione elettronica utilizzate per la fornitura di servizi di comunicazione al pubblico online;

(...)».

21 L'articolo L. 331-15 di tale codice così recita:

«La [Hadopi] è composta da un collegio e da una commissione per la protezione dei diritti. (…) (...)

(...)

Nell'esercizio dei loro poteri, i membri del collegio e della commissione per la protezione dei diritti non ricevono istruzioni da nessuna autorità».

22 L'articolo L. 331-17, primo comma, dello stesso codice è così formulato:

«La commissione per la protezione dei diritti è incaricata di adottare le misure previste all'articolo L. 331-25».

23 L'articolo L. 331-21 del CPI così recita:

«Per l'esercizio dei suoi poteri da parte della commissione per la protezione dei diritti, la [Hadopi] si avvale di agenti pubblici giurati, autorizzati dal [suo] presidente alle condizioni stabilite per decreto adottato previo parere del Conseil d'État [Consiglio di Stato] (...). (...)

I membri della commissione per la protezione dei diritti e gli agenti menzionati nel primo comma ricevono i ricorsi indirizzati alla suddetta commissione alle condizioni previste dall'articolo L. 331-24 e svolgono l'esame dei fatti.

Essi possono ottenere, ai fini del procedimento, tutti i documenti, qualunque ne sia il supporto, compresi i dati conservati e trattati dagli operatori di comunicazioni elettroniche ai sensi dell'articolo L. 34-1 del code des postes et des communications électroniques [codice delle poste e delle comunicazioni elettroniche] e dai fornitori di servizi di cui all'articolo 6, I, paragrafi 1 e 2, della loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [legge n. 2004-575, del 21 giugno 2004, per la fiducia nell'economia digitale].

Essi possono, inoltre, ottenere copie dei documenti menzionati al comma precedente.

Essi possono, in particolare, ottenere dagli operatori di comunicazioni elettroniche l'identità, l'indirizzo postale, l'indirizzo di posta elettronica e i recapiti telefonici dell'abbonato il cui accesso a servizi di comunicazione al pubblico online è stato utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere o oggetti protetti senza l'autorizzazione dei titolari dei diritti (…), laddove questa sia richiesta».

24 L'articolo L. 331-24 di detto codice così dispone:

«La commissione per la protezione dei diritti agisce su ricorso di agenti giurati e autorizzati (...) designati:

– dagli organismi di difesa professionale regolarmente costituiti;

– dagli organismi di gestione collettiva;

– dal Centre national du cinéma et de l'image animée (Centro nazionale della cinematografia e dell'immagine animata).

La commissione per la protezione dei diritti può parimenti agire sulla base di informazioni che le vengono trasmesse dal procuratore della Repubblica.

Essa non può essere investita di fatti risalenti a più di sei mesi».

25 Ai sensi dell'articolo L. 331-25 di tale codice, che disciplina la cosiddetta procedura di «risposta graduata»:

«Qualora essa sia investita di fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3 [del CPI], la commissione per la protezione dei diritti può inviare all'abbonato (...) una raccomandazione contenente richiamo alle disposizioni di cui all'articolo L. 336-3, con l'intimazione di rispettare l'obbligo da esse definito, e lo avverte in merito alle sanzioni previste ai sensi degli articoli L. 335-7 e L. 335-7-1. Tale raccomandazione contiene parimenti un'informazione dell'abbonato sull'offerta legale di contenuti culturali online, sull'esistenza di strumenti di messa in sicurezza che consentono di prevenire gli inadempimenti dell'obbligo definito all'articolo L. 336-3 nonché sui pericoli per il rinnovamento della creazione artistica e per l'economia del settore culturale generati dalle pratiche che non rispettano il diritto d'autore e i diritti connessi.

In caso di reiterazione, entro sei mesi a decorrere dall'invio della raccomandazione di cui al primo comma, di fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3, la commissione può inviare una nuova raccomandazione contenente le stesse informazioni della precedente per via elettronica (...). Essa deve allegare a tale raccomandazione una lettera consegnata contro firma o qualsiasi altro mezzo atto a provare la data di notifica di tale raccomandazione.

Le raccomandazioni inviate sulla base del presente articolo indicano la data e l'ora in cui i fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3 sono stati constatati. Per contro, esse non divulgano il contenuto delle opere o degli oggetti protetti interessati da tale violazione. Esse indicano i recapiti telefonici, postali ed elettronici ai quali il loro destinatario può inviare, se lo desidera, osservazioni alla commissione per la protezione dei diritti ed ottenere, qualora formuli una richiesta espressa in tal senso, precisazioni sul contenuto delle opere o degli oggetti protetti interessati dalla violazione addebitatagli».

26 L'articolo L. 331-29 del CPI dispone quanto segue:

«La [Hadopi] è autorizzata a creare un trattamento automatizzato dei dati personali per le persone che sono oggetto di un procedimento ai sensi della presente sottosezione.

Tale trattamento è diretto all'attuazione, da parte della commissione per la protezione dei diritti, delle misure previste dalla presente sottosezione, di tutti gli atti procedimentali connessi e delle modalità di informazione, nei confronti degli organismi di difesa professionale e degli organismi di gestione collettiva, degli eventuali ricorsi all'autorità giudiziaria e delle notifiche previste al quinto comma dell'articolo L. 335-7.

Un decreto (...) stabilisce le modalità di applicazione del presente articolo. Esso specifica in particolare:

– le categorie di dati registrati e il loro periodo di conservazione;

– i destinatari autorizzati a ricevere la comunicazione di tali dati, in particolare le persone la cui attività consiste nell'offrire accesso a servizi di comunicazione al pubblico online;

– le condizioni alle quali le persone interessate possono esercitare il loro diritto di accesso ai dati che li riguardano presso la [Hadopi] (...)».

27 L'articolo L. 335-2, commi primo e secondo, di tale codice precisa quanto segue:

«Ogni edizione di scritti, di composizione musicale, di disegno, di pittura o di qualsiasi altra produzione, stampata o incisa in tutto o in parte, in violazione delle leggi e dei regolamenti relativi alla proprietà degli autori, è una contraffazione e ogni contraffazione costituisce reato (délit).

La contraffazione in Francia di opere pubblicate in Francia o all'estero è punita con tre anni di reclusione e una multa di EUR 300 000 euro».

28 L'articolo L. 335-4, primo comma, di detto codice enuncia quanto segue:

«È punito con tre anni di reclusione e con multa di EUR 300 000 qualsiasi fissazione, riproduzione, comunicazione o messa a disposizione del pubblico, a titolo oneroso o gratuito, o qualsiasi telediffusione di una prestazione, di un fonogramma, di un videogramma, di un programma o di una pubblicazione di stampa, realizzata senza l'autorizzazione, quando essa è richiesta, dell'artista interprete, del produttore di fonogrammi o di videogrammi, dell'impresa di comunicazione audiovisiva, dell'editore o dell'agenzia di stampa».

29 L'articolo L. 335-7 del CPI detta le norme relative all'irrogazione alle persone colpevoli dei reati di cui in particolare agli articoli L. 335-2 e L. 335-4 di tale codice della pena accessoria della sospensione dell'accesso a un servizio di comunicazione al pubblico online per una durata massima di un anno.

30 L'articolo L. 335-7-1, primo comma, di detto codice così recita:

«Per le contravvenzioni della quinta classe previste dal presente codice, ove previsto dal regolamento, in caso di negligenza grave può essere irrogata, con le stesse modalità, la pena accessoria definita all'articolo L. 335-7 nei confronti del titolare dell'accesso ad un servizio di comunicazione al pubblico online al quale la commissione per la protezione dei diritti, in applicazione dell'articolo L. 331-25, abbia previamente inviato, mediante lettera consegnata contro firma o qualsiasi altro mezzo atto a provare la data di notifica della raccomandazione, una raccomandazione che lo inviti ad attuare un mezzo di sicurezza del suo accesso a Internet».

31 Ai sensi dell'articolo L. 336-3 dello stesso codice:

«Il titolare dell'accesso a servizi di comunicazione al pubblico online è tenuto ad assicurare che tale accesso non sia utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere od oggetti protetti dal diritto d'autore o da un diritto connesso senza l'autorizzazione dei titolari (…) laddove questa sia richiesta.

La violazione da parte del titolare dell'accesso dell'obbligo definito al primo comma non comporta il sorgere della responsabilità penale dell'interessato (...)».

32 L'articolo R. 331-37, primo comma, del CPI prevede quanto segue:

«Gli operatori di comunicazioni elettroniche [...] e i fornitori di servizi [...] sono tenuti a comunicare, mediante interconnessione al trattamento automatizzato dei dati personali di cui all'articolo L. 331-29 o mediante un supporto di registrazione che garantisca la loro integrità e sicurezza, i dati personali e le informazioni di cui al punto 2 dell'allegato del [décret n. 2010–236 (decreto n. 2010 236)] entro un termine di otto giorni dalla trasmissione, da parte della commissione per la protezione dei diritti, dei dati tecnici necessari all'identificazione dell'abbonato il cui accesso a servizi di comunicazione al pubblico online è stato utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere o oggetti protetti senza l'autorizzazione dei titolari dei diritti (…) laddove questa sia richiesta».

33 L'articolo R. 331-40 di tale codice così recita:

«La commissione per la tutela dei diritti, allorché, entro un anno dalla presentazione della raccomandazione di cui all'articolo L. 335-7-1, primo comma, le sono sottoposti nuovi fatti idonei ai costituire una negligenza grave ai sensi dell'articolo R. 335-5, informa l'abbonato, mediante lettera consegnata contro firma, che tali fatti sono idonei ad essere perseguiti. La lettera invita l'interessato a presentare le sue osservazioni entro un termine di quindici giorni. Essa precisa che l'interessato può, entro lo stesso termine, richiedere un'audizione ai sensi dell'articolo L. 331-21-1 e ha il diritto di essere assistito da un avvocato. Lo invita inoltre a precisare i suoi carichi familiari e le sue risorse.

La commissione può convocare l'interessato per un'audizione di propria iniziativa. La lettera di convocazione precisa che egli ha diritto di farsi assistere da un avvocato».

34 L'articolo R. 335-5 del CPI dispone quanto segue:

«I.- Costituisce una negligenza grave, punita con l'ammenda prevista per le contravvenzioni della quinta classe, il fatto, senza motivo legittimo, per la persona titolare di un accesso a servizi di comunicazione al pubblico online, qualora ricorrano le condizioni previste *sub* II:

1° o di non avere predisposto uno strumento di messa in sicurezza di tale accesso;

2° o di avere mancato di diligenza nell'attuazione di tale strumento.

II. – Le disposizioni sub I si applicano solo qualora ricorrano le due condizioni seguenti:

1° In applicazione dell'articolo L. 331-25 e nelle forme previste da tale articolo, la commissione per la protezione dei diritti abbia raccomandato al titolare dell'accesso l'attuazione di uno strumento di messa in sicurezza del suo accesso che consenta di prevenire la reiterazione di un uso del medesimo al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere od oggetti protetti dal diritto d'autore o da un diritto connesso senza l'autorizzazione dei titolari dei diritti (...) laddove questa sia richiesta;

2° Nell'anno successivo alla presentazione di tale raccomandazione, siffatto accesso venga nuovamente utilizzato ai fini menzionati al punto 1 del presente paragrafo II».

35 Dal 1° gennaio 2022, ai sensi della loi n° 2021-1382, du 25 octobre 2021, relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (legge n. 2021-1382 del 25 ottobre 2021 sulla regolamentazione e la protezione dell'accesso alle opere culturali nell'era digitale) (JORF n. 250 del 26 ottobre 2021, testo n. 2), l'Hadopi si è fusa con il Conseil supérieur de l'audiovisuel (Consiglio superiore dell'audiovisivo, CSA), altra autorità pubblica indipendente, per formare l'Autorité de régulation de la communication audiovisuelle et numérique (Autorità di regolamentazione della comunicazione audiovisiva e digitale, ARCOM).

36 La procedura di risposta graduata di cui al punto 25 della presente sentenza è rimasta tuttavia sostanzialmente invariata, anche se oramai non viene condotta dalla commissione per la tutela dei diritti dell'Hadopi, che era composta da tre membri nominati rispettivamente dal Conseil d'État (Consiglio di Stato), dalla Cour des Comptes (Corte dei conti) e dalla Corte di Cassazione, ma da due membri del collegio dell'ARCOM, uno dei quali è nominato dal Consiglio di Stato e l'altro dalla Cour de cassation (Corte di Cassazione).

Decreto n. 2010-236

37 L'articolo 1 del decreto n. 2010-236, emanato sulla base dell'articolo L. 331-29 del CPI, stabilisce quanto segue:

«Il trattamento di dati personali denominato "Sistema di gestione delle misure per la protezione delle opere su Internet" ha per finalità l'attuazione, da parte della commissione per la protezione dei diritti della [Hadopi]:

1° delle misure previste dal libro III della parte legislativa del [CPI] (titolo III, capo 1, sezione 3, sottosezione 3) e dal libro III della parte regolamentare dello stesso codice (titolo III, capo I, sezione 2, sottosezione 2);

2° dei ricorsi al procuratore della Repubblica relativi a fatti idonei a costituire reati previsti agli articoli L. 335-2, L. 335-3, L. 335-4 e R. 335-5 dello stesso codice, nonché dell'informazione degli organismi di difesa professionale e degli organismi di gestione collettiva di tali ricorsi;

(...)».

38 L'articolo 4 di tale decreto dispone quanto segue:

«I.– Hanno accesso diretto ai dati personali e alle informazioni menzionate all'allegato al presente decreto gli agenti pubblici giurati autorizzati dal presidente della [Hadopi] in applicazione dell'articolo

L. 331-21 del [CPI] e i membri della commissione per la protezione dei diritti menzionata all'articolo 1.

II.– Gli operatori di comunicazioni elettroniche e i fornitori di servizi menzionati al punto 2 dell'allegato al presente decreto sono destinatari:

– dei dati tecnici necessari all'identificazione dell'abbonato;

– delle raccomandazioni previste all'articolo L. 331-25 del [CPI] ai fini del loro invio per via elettronica ai loro abbonati;

– degli elementi necessari all'attuazione delle pene accessorie della sospensione dell'accesso ad un servizio di comunicazione al pubblico online portate a conoscenza della commissione per la protezione dei diritti da parte del procuratore della Repubblica.

III.– Gli organismi di difesa professionale e gli organismi di gestione collettiva sono informati dell'adizione del procuratore della Repubblica.

IV.– Le autorità giudiziarie sono destinatarie dei verbali di accertamento di fatti idonei a costituire reati previsti agli articoli L. 335-2, L. 335-3, L. 335-4, L. 335-7, R. 331-37, R. 331-38 e R. 335-5 del [CPI].

Il casellario giudiziale automatizzato è informato dell'esecuzione della pena della sospensione».

39 L'allegato a detto decreto così prevede:

«I dati personali e le informazioni registrate nel trattamento denominato "Sistema di gestione delle misure per la protezione delle opere su Internet" sono i seguenti:

1° Dati personali e informazioni provenienti dagli organismi di difesa professionale regolarmente costituiti, dagli organismi di gestione collettiva, dal Centro nazionale della cinematografia e dell'immagine animata, nonché quelli provenienti dal procuratore della Repubblica:

Quanto ai fatti idonei a costituire una violazione dell'obbligo definito all'articolo L. 336-3 del [CPI]:

Data e ora dei fatti;

Indirizzo IP degli abbonati interessati;

Protocollo peer-to-peer utilizzato;

Pseudonimo utilizzato dall'abbonato;

Informazioni relative alle opere o agli oggetti protetti interessati dai fatti;

Nome del file come presente sulla stazione dell'abbonato (se del caso);

Fornitore di accesso ad Internet presso il quale l'accesso è stato sottoscritto o che ha fornito la risorsa tecnica IP.

(...)

2° Dati personali ed informazioni relative all'abbonato raccolte presso operatori di comunicazioni elettroniche (...) e fornitori di servizi (...):

Cognome, nomi;

Indirizzo postale e indirizzi di posta elettronica;

Recapiti telefonici;

Indirizzo dell'impianto telefonico dell'abbonato;

Fornitore di accesso ad Internet, che utilizza le risorse tecniche del fornitore di accesso menzionato al punto 1°, presso il quale l'abbonato ha sottoscritto il suo contratto; numero di pratica;

Data di inizio della sospensione dell'accesso ad un servizio di comunicazione al pubblico online.

(...)».

Codice delle poste e delle comunicazioni elettroniche

40 L'articolo L. 34-1, II bis, del Codice delle poste e delle comunicazioni elettroniche così prevede:

«Gli operatori di comunicazioni elettroniche sono tenuti a conservare:

1° Ai fini dei procedimenti penali, della prevenzione delle minacce alla pubblica sicurezza e della salvaguardia della sicurezza nazionale, le informazioni relative all'identità anagrafica dell'utente, fino alla scadenza del termine di cinque anni dalla fine della validità del suo contratto;

2° Per gli stessi scopi di cui al punto 1° del presente paragrafo II bis, le altre informazioni fornite dall'utente al momento della sottoscrizione di un contratto o della creazione di un conto nonché le informazioni relative al pagamento, fino alla scadenza del termine di un anno a decorrere dalla fine della validità del suo contratto o dalla chiusura del suo conto;

3° Ai fini della lotta alla criminalità e ai reati gravi, della prevenzione delle minacce gravi alla pubblica sicurezza e della salvaguardia della sicurezza nazionale, i dati tecnici che consentano di identificare l'origine della connessione o quelli relativi alle apparecchiature terminali impiegate, fino alla scadenza del termine di un anno dalla connessione o dall'impiego delle apparecchiature terminali».

Procedimento principale e questioni pregiudiziali

41 Avendo il Premier ministre (Primo Ministro, Francia) implicitamente respinto la loro domanda diretta all'abrogazione del decreto n. 2010-236, le ricorrenti nel procedimento principale, con atto introduttivo del 12 agosto 2019, hanno adito il Conseil d'État (Consiglio di Stato, Francia) con un ricorso diretto all'annullamento di tale decisione implicita di rigetto. Esse hanno fatto valere, in sostanza, che l'articolo L. 331-21, commi dal terzo al quinto, del CPI – che fa parte della base giuridica di tale decreto – da un lato, è contrario al diritto al rispetto della vita privata sancito dalla Costituzione francese e, dall'altro, viola il diritto dell'Unione, in particolare l'articolo 15 della direttiva 2002/58 nonché gli articoli 7, 8, 11 e 52 della Carta.

42 Per quanto riguarda l'aspetto del ricorso relativo all'asserita violazione della Costituzione, il Conseil d'État (Consiglio di Stato) ha investito il Conseil constitutionnel (Consiglio costituzionale, Francia) di una questione prioritaria di legittimità costituzionale.

43 Con decisione n. 2020-841 QPC del 20 maggio 2020, La Quadrature du Net et autres [Diritto di comunicazione alla Hadopi], il Conseil constitutionnel (Consiglio costituzionale) ha dichiarato contrari alla Costituzione i commi terzo e quarto dell'articolo L. 331-21 del CPI, ma ha dichiarato conforme ad essa il quinto comma di detto articolo ad eccezione dell'espressione «in particolare» ivi contenuta.

44 Per quanto riguarda l'aspetto del ricorso relativo all'asserita violazione del diritto dell'Unione, le ricorrenti nel procedimento principale hanno sostenuto, in particolare, che il decreto n. 2010-236 e le disposizioni che ne costituiscono la base giuridica autorizzano un accesso sproporzionato a dati di connessione per reati relativi al diritto d'autore commessi su Internet e non gravi, senza un controllo previo da parte di un giudice o di un'autorità che offra garanzie di indipendenza e d'imparzialità. In particolare, tali reati non rientrerebbero nella «criminalità grave» oggetto della sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970).

45 A tal riguardo, il Conseil d'État (Consiglio di Stato) ricorda, da un lato, che, con la sentenza del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), la Corte ha

dichiarato, in particolare, che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non osta a misure legislative che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alla criminalità e di salvaguardia della sicurezza pubblica, una conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica. Pertanto, per quanto riguarda i dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, siffatta conservazione di tali dati sarebbe possibile, senza un termine particolare, a fini generali di ricerca, accertamento e perseguimento dei reati. La direttiva 2002/58 non osterebbe neppure ad un accesso a tali dati a detti fini.

46 Il giudice del rinvio ne desume che, per quanto riguarda l'accesso a dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, dovrebbe essere respinto il motivo dei ricorrenti nel procedimento principale relativo all'illegittimità del decreto n. 2010-236, in quanto quest'ultimo è stato adottato per contrastare reati non gravi.

47 Tale giudice ricorda, d'altro lato, che la Corte, nella sua sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970), ha dichiarato, in particolare, che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8, 11, e dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza sottoporre detto accesso ad un controllo previo da parte di un giudice o di un organismo amministrativo indipendente.

48 Il giudice del rinvio fa riferimento, più specificamente, al punto 120 di tale sentenza, nel quale la Corte ha precisato che è essenziale che un accesso siffatto ai dati conservati sia subordinato, in linea di principio, salvo casi di urgenza debitamente giustificati, al requisito di un controllo previo effettuato o da un giudice o da un'entità amministrativa indipendente, e che la decisione di tale giudice o di tale entità avvenga a seguito di una richiesta motivata delle autorità suddette, presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale.

49 La Corte avrebbe ribadito detto requisito nella sentenza del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), per quanto riguarda la raccolta in tempo reale dei dati di connessione da parte dei servizi di intelligence, e nella sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche) (C-746/18, EU:C:2021:152), per quanto riguarda l'accesso delle autorità nazionali ai dati di connessione.

50 Il giudice del rinvio osserva altresì che, a partire dalla sua creazione nel corso del 2009, la Hadopi ha inviato oltre 12,7 milioni di raccomandazioni a titolari di abbonamenti nell'ambito della procedura di risposta graduata prevista all'articolo L. 331-25 del CPI, di cui 827 791 nel corso del solo anno 2019. Tale circostanza implicherebbe che gli agenti della commissione per la tutela dei diritti della Hadopi abbiano dovuto necessariamente raccogliere, ogni anno, un numero considerevole di dati relativi all'identità civile degli utenti interessati. Esso ritiene che, tenuto conto del volume di tali raccomandazioni, il fatto di sottoporre tale raccolta a un controllo previo rischierebbe di rendere impossibile l'attuazione delle suddette raccomandazioni.

51 È in tali circostanze che il Conseil d'État (Consiglio di Stato) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se i dati relativi all'identità civile corrispondenti a un indirizzo IP rientrino tra i dati di traffico o di ubicazione soggetti, in linea di principio, a un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente con poteri vincolanti.

2) In caso di risposta affermativa alla prima questione e tenuto conto della bassa sensibilità dei dati relativi all'identità civile degli utenti, compresi i loro recapiti, si pone la questione di stabilire se la direttiva [2002/58], letta alla luce della [Carta], debba essere interpretata nel senso che essa osta a una normativa nazionale che prevede la raccolta di tali dati relativi agli indirizzi IP degli utenti da parte di un'autorità amministrativa, senza un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente con poteri vincolanti.

3) In caso di risposta affermativa alla seconda questione e tenuto conto della bassa sensibilità dei dati relativi all'identità civile, del fatto che solo tali dati possono essere raccolti al solo scopo di prevenire violazioni di obblighi definiti in modo circostanziato, restrittivo e limitativo dal diritto nazionale, e del fatto che un controllo sistematico dell'accesso ai dati di ogni utente da parte di un giudice o di un'entità amministrativa terza con poteri vincolanti sarebbe tale da compromettere l'espletamento della missione di servizio pubblico affidata all'autorità amministrativa anch'essa indipendente che effettua tale raccolta, si pone la questione di stabilire se la direttiva [2002/58] osti allo svolgimento di tale controllo con modalità appropriate, come un controllo automatizzato, eventualmente sotto la supervisione di un servizio interno all'organismo, che offra garanzie di indipendenza e di imparzialità relativamente agli agenti incaricati di tale raccolta».

Sulle questioni pregiudiziali

52 Con le sue tre questioni pregiudiziali, che è opportuno esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che osta a una normativa nazionale che autorizza l'autorità pubblica, incaricata della protezione dei diritti d'autore e dei diritti connessi contro le violazioni di tali diritti commesse su Internet, ad accedere ai dati relativi all'identità civile, conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico, corrispondenti a indirizzi IP precedentemente raccolti da organismi degli aventi diritto, affinché tale autorità pubblica possa identificare i titolari di tali indirizzi, utilizzati per attività che possono costituire violazioni di tal genere, e possa adottare, se del caso, misure nei loro confronti, senza che detto accesso sia subordinato al requisito di un previo controllo da parte di un giudice o di un organismo amministrativo indipendente.

Osservazioni preliminari

53 Nel procedimento principale sono in discussione due trattamenti di dati personali distinti e successivi che avvengono nell'ambito delle attività della Hadopi, autorità pubblica indipendente, il cui compito consiste, in particolare, conformemente all'articolo L. 331-13 del CPI, nella protezione delle opere e degli oggetti protetti dal diritto d'autore o da un diritto connesso contro violazioni di tali diritti commesse sulle reti di comunicazione elettronica utilizzate per la fornitura di servizi di comunicazione al pubblico online.

54 Il primo trattamento, effettuato a monte da agenti giurati autorizzati di organismi degli aventi diritto, si svolge in due tempi. In un primo tempo, sono raccolti sulle reti tra pari (peer to peer) indirizzi IP che appaiono essere stati utilizzati per attività che possono costituire una violazione di un diritto d'autore o di un diritto connesso. In un secondo tempo, è messo a disposizione dell'Hadopi sotto forma di verbali un insieme di dati personali e informazioni. Tali dati sono, secondo l'elenco di cui al punto 1º dell'allegato al decreto n. 2010-236, la data e l'ora dei fatti, l'indirizzo IP degli abbonati interessati, il protocollo tra pari (peer to peer) utilizzato, lo pseudonimo utilizzato dall'abbonato, le informazioni relative alle opere o oggetti protetti interessati dai fatti, il nome del file come presente sulla stazione dell'abbonato (se del caso), e il fornitore di accesso a Internet presso il quale è stato sottoscritto l'accesso o che ha fornito la risorsa tecnica IP.

55 Il secondo trattamento, effettuato a valle dai fornitori di accesso a Internet su richiesta dell'Hadopi, si svolge anch'esso in due tempi. In un primo tempo, gli indirizzi IP raccolti a monte sono messi in relazione con i titolari di tali indirizzi. In un secondo momento, è messo a disposizione di tale autorità pubblica un insieme di dati personali e informazioni relativi a detti titolari, vertenti essenzialmente sulla loro identità civile. Tali dati, secondo l'elenco di cui al punto 2º dell'allegato al decreto n. 2010/236, sono essenzialmente il cognome e i nomi, l'indirizzo postale e gli indirizzi di posta elettronica, i recapiti telefonici nonché l'indirizzo dell'installazione telefonica dell'abbonato.

56 A quest'ultimo riguardo, l'articolo L. 331-21 del CPI prevede, al suo quinto comma, nella sua versione risultante dalla decisione del Conseil constitutionnel (Consiglio costituzionale) menzionata al punto 43 della presente sentenza, che i membri della commissione per la tutela dei diritti della Hadopi e i funzionari pubblici giurati di tale autorità, autorizzati dal suo presidente, possano ottenere dagli operatori di comunicazione elettronica l'identità, l'indirizzo postale, l'indirizzo di posta elettronica e i

recapiti telefonici dell'abbonato il cui accesso a servizi di comunicazione al pubblico online sia stato utilizzato al fine di riprodurre, rappresentare, mettere a disposizione o comunicare al pubblico opere o oggetti protetti senza l'autorizzazione dei titolari dei diritti, laddove questa sia richiesta.

57 Tali diversi trattamenti di dati personali mirano a consentire alla Hadopi di adottare, nei confronti dei titolari di indirizzi IP così identificati, le misure previste nell'ambito del procedimento amministrativo cosiddetto di «risposta graduata» disciplinato dall'articolo L. 331-25 del CPI. Tali misure sono, anzitutto, l'invio di «raccomandazioni», assimilabili ad avvertimenti; in secondo luogo, in caso di adizione della Commissione per i diritti della Hadopi entro un anno dall'invio di una seconda raccomandazione, per fatti che possono costituire una reiterazione della violazione accertata, l'informazione diretta all'abbonato, di cui all'articolo R. 331-40 del CPI, riguardo al fatto che i fatti sono idonei a configurare il cosiddetto reato di «negligenza grave», definito all'articolo R. 335-5 del CPI, contravvenzione punita con una ammenda massima di EUR 1 500 e di EUR 3 000 in caso di recidiva; infine, previa delibera, l'adizione del pubblico ministero per fatti che possono costituire una contravvenzione siffatta o, se del caso, il reato (délit) di contraffazione di cui all'articolo L. 335-2 del CPI o all'articolo L. 335-4 di tale codice, punito con tre anni di reclusione e con multa di EUR 300 000.

58 Ciò premesso, le questioni sollevate dal giudice del rinvio riguardano unicamente il trattamento a valle descritto al punto 55 della presente sentenza e non il trattamento a monte le cui caratteristiche essenziali sono state esposte al punto 54 della medesima sentenza.

59 Occorre tuttavia rilevare che, qualora la previa raccolta degli indirizzi IP da parte degli organismi degli aventi diritto interessati fosse contraria al diritto dell'Unione, quest'ultimo diritto osterebbe parimenti alla gestione di tali dati nell'ambito del trattamento successivo da parte dei fornitori di servizi di comunicazione elettronica consistente nel mettere in relazione detti indirizzi con i dati relativi all'identità civile dei titolari di questi stessi indirizzi.

60 In detto contesto, va notato fin da subito che, secondo la giurisprudenza della Corte, gli indirizzi IP costituiscono sia dati sul traffico ai fini della direttiva 2002/58 sia dati personali ai fini del RGPD (v., in tal senso, sentenza del 17 giugno 2021, M.I.C.M., C-597/19, EU:C:2021:492, punti 102 e 113 e giurisprudenza ivi citata).

61 Tuttavia, la raccolta di indirizzi IP, pubblici e visibili per tutti, da parte di agenti di organismi degli aventi diritto non rientra nell'ambito di applicazione della direttiva 2002/58, poiché un trattamento siffatto non è manifestamente «connesso alla fornitura di servizi di comunicazione elettronica», ai sensi dell'articolo 3 di tale direttiva.

62 Per contro, siffatta raccolta di indirizzi IP, autorizzata, come risulta dal fascicolo a disposizione della Corte, entro determinati limiti quantitativi e a determinate condizioni, dalla Commission nationale de l'informatique et des libertés (CNIL) [Commissione nazionale per l'informatica e le libertà (CNIL), Francia], ai fini della loro trasmissione all'Hadopi per il loro eventuale utilizzo in procedimenti amministrativi o giurisdizionali successivi volti a lottare contro le attività lesive dei diritti d'autore e dei diritti connessi, costituisce un «trattamento», ai sensi dell'articolo 4, punto 2, del RGPD, la cui liceità dipende dalle condizioni poste dall'articolo 6, paragrafo 1, primo comma, lettera f), di tale regolamento, alla luce della giurisprudenza della Corte elaborata in particolare nelle sentenze del 17 giugno 2021, M.I.C.M. (C-597/19, EU:C:2021:492, punti 102 e 103), nonché del 4 luglio 2023, Meta Platforms e a. (Condizioni generali di utilizzo di un social network) (C-252/21, EU:C:2023:537, punti da 106 a 112 e giurisprudenza ivi citata).

63 Per quanto riguarda il trattamento a valle descritto al punto 55 della presente sentenza, esso rientra, dal canto suo, nell'ambito di applicazione della direttiva 2002/58 poiché è «connesso alla fornitura di servizi di comunicazione elettronica», ai sensi dell'articolo 3 di tale direttiva, purché i dati di cui trattasi siano ottenuti dai fornitori di servizi di comunicazione elettronica conformemente all'articolo L. 331-21 del CPI.

Sull'esistenza di una giustificazione, ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, dell'accesso di un'autorità pubblica a dati relativi all'identità civile corrispondenti a un indirizzo IP conservati dai fornitori di servizi di comunicazione elettronica ai fini della lotta contro la contraffazione commessa online

64 Alla luce delle osservazioni preliminari che precedono, si pone la questione se, come si chiede il giudice del rinvio, la limitazione dei diritti fondamentali sanciti agli articoli 7, 8 e 11 della Carta, comportata dall'accesso da parte di un'autorità pubblica, come la Hadopi, a dati relativi all'identità civile corrispondenti a un indirizzo IP di cui essa già dispone, possa essere giustificata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58.

65 Ebbene, l'accesso a tali dati può essere concesso soltanto se e in quanto essi siano stati conservati da detti fornitori in un modo conforme alla direttiva 2002/58 [v., in tal senso, sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 29].

Sui requisiti relativi alla conservazione dei dati relativi all'identità civile e degli indirizzi IP corrispondenti da parte dei fornitori di servizi di comunicazione elettronica

66 L'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di principio, enunciato all'articolo 5, paragrafo 1, di tale direttiva, di garantire la riservatezza dei dati personali nonché ai corrispondenti obblighi, menzionati in particolare agli articoli 6 e 9 di detta direttiva, qualora siffatta restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa e della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine, gli Stati membri possono, tra l'altro, adottare misure legislative che prevedano la conservazione dei dati per un periodo di tempo limitato, qualora ciò sia giustificato da uno dei suddetti motivi. Ciò premesso, la facoltà di derogare ai diritti e agli obblighi previsti dagli articoli 5, 6 e 9 della direttiva 2002/58 non può giustificare che la deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati e, in particolare, al divieto di memorizzare tali dati, espressamente previsto all'articolo 5 di detta direttiva, divenga la regola (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 110 e 111).

67 Una misura legislativa adottata ai sensi di tale disposizione deve, pertanto, rispondere effettivamente e rigorosamente a uno degli obiettivi menzionati al punto precedente, dato che l'elenco di questi ultimi all'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 ha carattere esaustivo, e rispettare i principi generali del diritto dell'Unione, tra i quali figura il principio di proporzionalità, e dei diritti fondamentali garantiti dalla Carta. A tal riguardo, la Corte ha già dichiarato che l'obbligo imposto da uno Stato membro ai fornitori di servizi di comunicazione elettronica, in forza di una normativa nazionale, di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto non soltanto degli articoli 7 e 8 della Carta, relativi, rispettivamente, alla tutela della vita privata e alla protezione dei dati personali, ma anche dell'articolo 11 della Carta, relativo alla libertà di espressione (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 112 e 113).

68 Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/85 deve tenere conto dell'importanza sia del diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto alla protezione dei dati personali, sancito dall'articolo 8 di quest'ultima, quale emerge dalla giurisprudenza della Corte, nonché del diritto alla libertà di espressione, dal momento che tale diritto fondamentale, garantito dall'articolo 11 della Carta, costituisce uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 114 e giurisprudenza citata).

69 Occorre sottolineare, a tale proposito, che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce, di per sé, da un lato, una deroga al divieto, previsto dall'articolo 5, paragrafo 1, della direttiva 2002/58, per qualsiasi persona diversa dagli utenti di memorizzare tali dati e, dall'altro, un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta, a prescindere dalla circostanza che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza. È del pari irrilevante la

circostanza che i dati conservati siano o meno utilizzati successivamente, in quanto l'accesso a tali dati costituisce, a prescindere dall'uso che ne viene fatto in seguito, un'ingerenza distinta nei diritti fondamentali indicati al punto precedente (sentenza del 6 ottobre 2020 nelle cause riunite C-511/18, C-512/18 e C-520/18 La Quadrature du Net e a., EU:C:2020:791, punti 115 e 116).

70 Ciò premesso, l'articolo 15, paragrafo 1, della direttiva 2002/58, là dove consente agli Stati membri di introdurre talune misure in deroga, com'è stato menzionato al punto 66 della presente sentenza, riflette la circostanza che i diritti sanciti dagli articoli 7, 8 e 11 della Carta non appaiono come prerogative assolute, ma devono essere presi in considerazione alla luce della loro funzione sociale. Come risulta, infatti, dall'articolo 52, paragrafo 1, della Carta, quest'ultima ammette limitazioni all'esercizio dei summenzionati diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 120 e 121).

71 Nel caso di specie, occorre rilevare che, sebbene formalmente la Hadopi sia autorizzata ad accedere soltanto ai dati relativi all'identità civile corrispondenti a un indirizzo IP, tale accesso presenta la particolarità che esso richiede, in via preliminare, che i fornitori di servizi di comunicazione elettronica considerati mettano in relazione l'indirizzo IP e i dati relativi all'identità civile del suo titolare. Detto accesso presuppone quindi necessariamente che i fornitori dispongano degli indirizzi IP nonché dei dati relativi all'identità dei loro titolari.

72 Inoltre, tale autorità pubblica cerca di ottenere l'accesso a tali dati al solo scopo di identificare il titolare di un indirizzo IP utilizzato per attività idonee a ledere i diritti d'autore o i diritti connessi, allorché quegli ha illegittimamente messo a disposizione su Internet opere protette per essere scaricate da altre persone. In tali circostanze, i dati relativi all'identità civile devono essere considerati strettamente connessi sia all'indirizzo IP sia alle informazioni relative all'opera messa a disposizione su Internet di cui dispone la Hadopi.

73 Ebbene, non si può prescindere da un siffatto contesto particolare nell'ambito dell'esame dell'eventuale giustificazione di una misura di conservazione di dati personali ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, interpretato alla luce degli articoli 7, 8 e 11 della Carta (v., per analogia, Corte EDU, 24 aprile 2018, Benedik c. Slovenia, CE:ECHR:2018:0424JUD006235714, § 109).

74 Pertanto, è alla luce dei requisiti derivanti, in materia di conservazione di indirizzi IP, da detto articolo 15, paragrafo 1, interpretato alla luce degli articoli 7, 8 e 11 della Carta, che occorre esaminare un'eventuale giustificazione dell'ingerenza nei diritti fondamentali, sanciti da questi ultimi articoli della Carta, comportata dalla conservazione, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, dei dati ai quali l'Hadopi ha un potere di accesso.

75 In tale contesto, occorre rilevare che, secondo la giurisprudenza della Corte, pur se, come ricordato al punto 60, gli indirizzi IP costituiscono dati relativi al traffico ai fini della direttiva 2002/58, tali indirizzi si distinguono dalle altre categorie di dati relativi al traffico nonché dai dati relativi all'ubicazione.

76 A tal riguardo, la Corte ha rilevato che gli indirizzi IP sono generati senza essere collegati a una comunicazione determinata e servono principalmente a identificare, tramite i fornitori di servizi di comunicazione elettronica, la persona fisica proprietaria di un'apparecchiatura terminale a partire dalla quale viene effettuata una comunicazione via Internet. Pertanto, in materia di posta elettronica e di telefonia via Internet, purché siano conservati solo gli indirizzi IP dell'origine della comunicazione e non quelli del destinatario della stessa, detti indirizzi non rivelano, in quanto tali, alcuna informazione sui terzi che sono stati in contatto con la persona all'origine della comunicazione. In tali limiti, detta categoria di dati presenta quindi un grado di sensibilità inferiore rispetto agli altri dati relativi al traffico (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 152).

77 È vero che, al punto 156 della sentenza del 6 ottobre 2020 nella causa La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), la Corte ha affermato che, nonostante la

constatazione che gli indirizzi IP sono meno sensibili quando sono utilizzati esclusivamente per identificare l'utente di un servizio di comunicazione elettronica, l'articolo 15, paragrafo 1, della direttiva 2002/58 osta alla conservazione generalizzata e indifferenziata dei soli indirizzi IP attribuiti all'origine di una connessione per finalità diverse dalla lotta alle forme gravi di criminalità e la prevenzione delle minacce gravi alla sicurezza pubblica o la salvaguardia della sicurezza nazionale. Tuttavia, la Corte, per giungere a tale conclusione, si è espressamente fondata sul carattere grave dell'ingerenza nei diritti fondamentali sanciti agli articoli 7, 8 e 11 della Carta che può comportare una siffatta conservazione degli indirizzi IP.

78 Al punto 153 della medesima sentenza, la Corte ha, infatti, considerato che, poiché gli indirizzi IP possono, quando sono utilizzati per effettuare il «tracciamento completo del percorso di navigazione di un utente di Internet» e, di conseguenza, della sua attività online, consentire segnatamente di tracciare il «profilo dettagliato» di tale utente, la conservazione e l'analisi di detti indirizzi IP necessari per un siffatto tracciamento costituiscono ingerenze gravi nei diritti fondamentali dell'interessato sanciti dagli articoli 7 e 8 della Carta, che possono avere effetti dissuasivi sull'esercizio, da parte degli utenti dei mezzi di comunicazione elettronica, della loro libertà di espressione, garantita dall'articolo 11 della Carta.

79 Occorre tuttavia sottolineare che qualsiasi conservazione generalizzata e indifferenziata di un insieme, eventualmente ampio, di indirizzi IP statici e dinamici utilizzati da una persona in un determinato periodo non costituisce necessariamente un'ingerenza grave nei diritti fondamentali garantiti dagli articoli 7, 8 e 11 della Carta.

80 A tal riguardo, anzitutto, le cause che hanno dato luogo alla sentenza del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), vertevano su normative nazionali che implicavano un obbligo di conservazione di un insieme di dati necessari per determinare la data, l'ora, la durata e il tipo della comunicazione, identificare il materiale di comunicazione utilizzato nonché localizzare le apparecchiature terminali e le comunicazioni, dati tra i quali comparivano, in particolare, il nome e l'indirizzo dell'utente, i numeri di telefono del chiamante e del chiamato nonché l'indirizzo IP per i servizi Internet. Inoltre, in due di tali cause, le normative nazionali in questione sembravano riguardare anche i dati relativi alla trasmissione delle comunicazioni elettroniche tramite le reti, e questi ultimi consentivano di individuare anche la natura delle informazioni consultate online (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 82 e 83).

81 La conservazione degli indirizzi IP effettuata nell'ambito di siffatte normative nazionali era quindi idonea, alla luce degli altri dati di cui tali normative imponevano la conservazione e della possibilità di combinare tali diversi dati, a consentire di trarre conclusioni precise sulla vita privata delle persone i cui dati erano interessati e, pertanto, a condurre a una grave ingerenza nei diritti fondamentali, sanciti agli articoli 7 e 8 della Carta, relativi alla protezione della vita privata e dei dati personali di tali persone, nonché all'articolo 11 di tale Carta, relativo alla libertà di espressione di queste ultime.

82 Per contro, l'obbligo imposto ai fornitori di servizi di comunicazione elettronica, da una misura legislativa ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, di garantire la conservazione generalizzata e indifferenziata degli indirizzi IP può, se del caso, essere giustificato dall'obiettivo della lotta contro i reati in generale, qualora sia escluso effettivamente che tale conservazione possa generare ingerenze gravi nella vita privata dell'interessato per effetto della possibilità di trarre conclusioni precise su quest'ultimo mediante, in particolare, un collegamento di tali indirizzi IP con un insieme di dati relativi al traffico o all'ubicazione che siano stati parimenti conservati da tali fornitori.

83 Pertanto, uno Stato membro che intenda imporre ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione generalizzata e indifferenziata degli indirizzi IP al fine di conseguire un obiettivo connesso alla lotta contro i reati in generale deve assicurarsi che le modalità di conservazione di detti dati siano tali da garantire che sia esclusa qualsiasi combinazione di detti indirizzi IP con altri dati conservati, nel rispetto della direttiva 2002/58, che consenta di trarre conclusioni precise sulla vita privata delle persone i cui dati siano così conservati.

84 Al fine di garantire che sia esclusa una combinazione di dati che consenta di trarre conclusioni precise sulla vita privata dell'interessato, le modalità di conservazione devono riguardare la struttura stessa

della conservazione che, in sostanza, deve essere organizzata in modo da garantire una separazione effettivamente stagna delle diverse categorie di dati conservati.

85 A tal riguardo, spetta certamente allo Stato membro, che intenda imporre ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione generalizzata e indifferenziata degli indirizzi IP al fine di conseguire un obiettivo connesso alla lotta contro i reati in generale, prevedere, nella sua normativa, norme chiare e precise relative a dette modalità di conservazione, modalità che devono rispondere a requisiti rigorosi. La Corte può tuttavia fornire precisazioni riguardo a tali modalità.

86 In primo luogo, le norme nazionali menzionate al punto precedente devono garantire che ciascuna categoria di dati, compresi i dati relativi all'identità civile e gli indirizzi IP, sia conservata in modo completamente separato dalle altre categorie di dati conservati.

87 In secondo luogo, tali norme devono garantire che, sul piano tecnico, mediante un dispositivo informatico sicuro e affidabile, sia effettivamente stagna la separazione delle diverse categorie di dati conservati, in particolare i dati relativi all'identità civile, gli indirizzi IP, i vari dati relativi al traffico diversi dagli indirizzi IP e i vari dati relativi all'ubicazione.

88 In terzo luogo, dette norme, nei limiti in cui prevedono la possibilità di mettere in relazione gli indirizzi IP conservati con l'identità civile della persona interessata nel rispetto dei requisiti derivanti dall'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 della Carta, devono consentire una siffatta messa in relazione solo mediante l'uso di un procedimento tecnico efficiente che non metta a rischio l'efficacia della separazione stagna di tali categorie di dati.

89 In quarto luogo, l'affidabilità di tale separazione stagna deve essere oggetto di un controllo regolare da parte di un'autorità pubblica diversa da quella che cerca di ottenere l'accesso ai dati personali conservati dai fornitori di servizi di comunicazione elettronica.

90 Purché, nella normativa nazionale applicabile, siano previsti siffatti rigorosi requisiti relativi alle modalità di conservazione generalizzata e indifferenziata degli indirizzi IP e degli altri dati conservati dai fornitori di servizi di comunicazione elettronica, l'ingerenza risultante da tale conservazione degli indirizzi IP non può, per effetto della struttura stessa di detta conservazione, essere qualificata come «grave».

91 Infatti, nel caso in cui sia istituito un dispositivo legislativo siffatto, le modalità di conservazione degli indirizzi IP così prescritte escludono che tali dati possano essere combinati con altri dati conservati nel rispetto della direttiva 2002/58, consentendo di trarre conclusioni precise sulla vita privata della persona interessata.

92 Di conseguenza, in presenza di un dispositivo legislativo che soddisfi i requisiti esposti ai punti da 86 a 89 della presente sentenza, che garantiscono che nessuna combinazione di dati consenta di trarre conclusioni precise sulla vita privata della persona considerata, l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 della Carta, non osta a che lo Stato membro interessato imponga un obbligo di conservazione generalizzata e indifferenziata degli indirizzi IP ai fini di un obiettivo di lotta contro i reati in generale.

93 Infine, come risulta dal punto 168 della sentenza del 6 ottobre 2020, La Quadrature du Net e a. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791), un quadro normativo del genere deve prevedere un periodo di conservazione limitato allo stretto necessario e assicurare, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongano di garanzie effettive contro i rischi di abuso nonché contro qualsiasi accesso a tali dati e qualsiasi uso illecito degli stessi.

94 Spetta al giudice del rinvio verificare se la normativa nazionale di cui trattasi nel procedimento principale rispetti i requisiti ricordati ai punti da 85 a 93 della presente sentenza.

Sui requisiti relativi all'accesso ai dati relativi all'identità civile corrispondente a un indirizzo IP conservati dai fornitori di servizi di comunicazione elettronica

95 Dalla giurisprudenza della Corte risulta che, nell'ambito della lotta contro i reati, soltanto gli obiettivi della lotta contro le forme gravi di criminalità o della prevenzione di gravi minacce per la sicurezza pubblica sono atti a giustificare l'ingerenza grave nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta che comporta l'accesso delle autorità pubbliche a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, suscettibili di fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali utilizzate da quest'ultimo e tali da permettere di trarre precise conclusioni sulla vita privata degli persone interessate, senza che altri fattori relativi alla proporzionalità di una domanda di accesso, quali la durata del periodo per il quale si chiede l'accesso a tali dati, possano avere come effetto che l'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale sia idoneo a giustificare un siffatto accesso [sentenza del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 35].

96 Per contro, qualora l'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta derivante dall'accesso delle autorità pubbliche ai dati relativi all'identità civile conservati dai fornitori di servizi di comunicazione elettronica, senza che tali dati possano essere associati ad informazioni relative alle comunicazioni effettuate, non sia grave poiché, considerati nel loro complesso, tali dati non consentono di trarre conclusioni precise riguardo alla vita privata delle persone i cui dati sono considerati, detto accesso può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati in generale (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punti 54, 57 e 60).

97 Occorre altresì aggiungere che, secondo un principio sancito da una giurisprudenza costante della Corte, l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione può essere giustificato in forza dell'articolo 15, paragrafo 1, della direttiva 2002/58 solo dall'obiettivo di interesse generale per il quale è stata imposta ai fornitori di servizi di comunicazione elettronica la loro conservazione, salvo che tale accesso sia giustificato da un obiettivo di interesse generale di maggiore importanza. Da tale principio discende in particolare che non può in alcun caso essere concesso un accesso siffatto a fini di lotta contro i reati in generale qualora la conservazione di detti dati sia stata giustificata dall'obiettivo di lotta contro la criminalità grave o, *a fortiori*, di salvaguardia della sicurezza nazionale (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 166).

98 Per contro, un siffatto obiettivo di lotta contro i reati in generale consente di giustificare che sia dato accesso ai dati relativi al traffico e all'ubicazione che sono stati memorizzati e quindi conservati nella misura e per la durata necessaria alla commercializzazione dei servizi, alla fatturazione e alla fornitura di servizi a valore aggiunto, come consentito dall'articolo 6 della direttiva 2002/58 (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punti 108 e 167).

99 Nel caso di specie, in primo luogo, dalla normativa nazionale oggetto del procedimento principale risulta che l'Hadopi non ha accesso a un «insieme di dati relativi al traffico o di dati relativi all'ubicazione» ai sensi della giurisprudenza citata al punto 95 della presente sentenza, per cui non può, in linea di principio, trarre conclusioni precise sulla vita privata delle persone interessate. Ebbene, un accesso che non consenta di trarre siffatte conclusioni non costituisce un'ingerenza grave nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta.

100 Infatti, secondo tale normativa e le spiegazioni fornite dal governo francese al riguardo, l'accesso concesso a detta autorità pubblica è strettamente limitato a taluni dati relativi all'identità civile del titolare di un indirizzo IP ed è autorizzato al solo fine di poter identificare tale titolare sospettato di aver svolto un'attività lesiva dei diritti d'autore o dei diritti connessi qualora abbia illegittimamente messo a disposizione su Internet opere protette, per poter essere scaricate da altre persone. Se del caso, tale accesso mira all'adozione nei confronti di tale titolare di uno dei provvedimenti pedagogici o repressivi previsti nell'ambito del procedimento di risposta graduata, vale a dire l'invio di una prima e di una seconda raccomandazione, poi di una lettera che gli notifica che tale attività può costituire un reato di negligenza grave e, infine, il ricorso al pubblico ministero per il perseguimento di tale contravvenzione o del reato (délit) di contraffazione.

101 Occorre altresì che detta normativa nazionale preveda norme chiare e precise idonee a garantire che gli indirizzi IP conservati nel rispetto della direttiva 2002/58 possano essere utilizzati unicamente per identificare la persona alla quale è stato assegnato un determinato indirizzo IP, escludendo al contempo un utilizzo che consenta di sorvegliare, mediante uno o più di tali indirizzi, l'attività online della persona interessata. Quando un indirizzo IP è quindi utilizzato al solo scopo di identificare il suo titolare nell'ambito di un procedimento amministrativo specifico che può sfociare in procedimenti penali nei confronti di tale titolare e non per fini diretti, ad esempio, a rivelare i contatti o l'ubicazione di tale titolare, l'accesso a tale indirizzo per quel solo scopo riguarda il suddetto indirizzo in quanto dato relativo all'identità civile e non in quanto dato relativo al traffico.

102 Per di più, dal principio sancito dalla giurisprudenza costante ricordata al punto 97 della presente sentenza discende che un accesso come quello di cui beneficia la Hadopi in forza della normativa nazionale oggetto del procedimento principale, poiché persegue l'obiettivo della lotta contro i reati in generale, può essere giustificato solo se verte su indirizzi IP che devono essere conservati dai fornitori di servizi di comunicazione elettronica ai fini di detto obiettivo e non ai fini di un obiettivo di maggiore rilevanza come quello della lotta contro la criminalità grave, fatto salvo tuttavia un accesso giustificato da un siffatto obiettivo di lotta contro i reati in generale allorché riguarda indirizzi IP memorizzati e quindi conservati alle condizioni previste dall'articolo 6 della direttiva 2002/58.

103 Inoltre, come risulta dai punti da 85 a 92 della presente sentenza, la conservazione di indirizzi IP, fondata su una misura legislativa ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58, con l'obiettivo della lotta contro i reati in generale, può essere giustificata qualora le modalità di tale conservazione istituite dal dispositivo legislativo interessato soddisfino un insieme di requisiti volti a garantire, in sostanza, una separazione effettivamente stagna delle diverse categorie di dati conservati, cosicché è effettivamente esclusa la combinazione di dati appartenenti a diverse categorie. Infatti, nel caso in cui tali modalità di conservazione siano imposte ai fornitori di servizi di comunicazione elettronica, una conservazione generalizzata e indifferenziata degli indirizzi IP non costituisce un'ingerenza grave nella vita privata dei loro titolari, poiché tali dati non consentono di trarre conclusioni precise sulla loro vita privata.

104 Pertanto, tenuto conto della giurisprudenza ricordata ai punti da 95 a 97 della presente sentenza, nel caso in cui sia attuato un dispositivo legislativo di questo tipo, l'accesso agli indirizzi IP conservati in vista dell'obiettivo della lotta contro i reati in generale può essere giustificato alla luce dell'articolo 15, paragrafo 1, della direttiva 2002/58 qualora tale accesso sia autorizzato al solo scopo di identificare la persona sospettata di essere implicata in tali reati.

105 Del resto, consentire a un'autorità pubblica, come la Hadopi, di avere accesso a dati relativi all'identità civile corrispondenti a un indirizzo IP pubblico che le è stato trasmesso da organismi degli aventi diritto al solo scopo di identificare il titolare di tale indirizzo utilizzato per attività, commesse online e idonee a violare i diritti d'autore o i diritti connessi, al fine dell'imposizione nei suoi confronti di una delle misure previste nell'ambito del procedimento di risposta graduata è conforme alla giurisprudenza della Corte relativa al «diritto d'informazione» nel contesto di un'azione relativa alla lesione di un diritto di proprietà intellettuale quale prevista all'articolo 8 della direttiva 2004/48 (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 47 e seguenti).

106 Infatti, nell'ambito di tale giurisprudenza, pur sottolineando che l'applicazione delle misure previste dalla direttiva 2004/48 non può porsi in contrasto con il RGPD né con la direttiva 2002/58, la Corte ha dichiarato che l'articolo 8, paragrafo 3, della direttiva 2004/48, in combinato disposto con l'articolo 15, paragrafo 1, della direttiva 2002/58 e l'articolo 7, lettera f), della direttiva 95/46, non osta a che gli Stati membri prevedano a carico dei fornitori di servizi di comunicazione elettronica l'obbligo di trasmissione a soggetti privati di dati personali per consentire l'avvio, dinanzi ai giudici civili, di procedimenti per perseguire le violazioni del diritto d'autore, senza peraltro imporre agli Stati medesimi di prevedere tale obbligo (v., in tal senso, sentenza del 17 giugno 2021, M.I.C.M., C-597/19, EU:C:2021:492, punti 124 e 125 e giurisprudenza ivi citata).

107 Ciò premesso, in secondo luogo, ai fini della valutazione concreta del grado di ingerenza nella vita privata comportata da un accesso di un'autorità pubblica a dati personali, non si può prescindere dalle specificità del contesto in cui tale accesso ha luogo e, in particolare, dall'insieme dei dati e delle

informazioni comunicati a tale autorità in forza della normativa nazionale applicabile, compresi i dati e le informazioni preesistenti rivelatori del contenuto (v., per analogia, Corte EDU, 24 aprile 2018, Benedik c. Slovenia, CE:ECHR:2018:0424JUD006235714, § 109).

108 Nel caso di specie, ai fini di tale valutazione occorre, pertanto, tener conto del fatto che, prima dell'accesso ai dati relativi all'identità civile di cui trattasi di cui beneficia, la Hadopi è destinataria da parte degli organismi degli aventi diritto, in particolare, delle «informazioni relative alle opere o agli oggetti protetti interessati dai fatti» e, «se del caso», il «nome del file come presente sulla stazione dell'abbonato», conformemente al punto 1º dell'allegato al decreto n. 2010-236.

109 Dal fascicolo di cui dispone la Corte, ma ferma restando la verifica da parte del giudice del rinvio, risulta che le informazioni sull'opera interessata, come riportate in un verbale il cui contenuto è disciplinato dalle delibere della CNIL, del 10 giugno 2010, si limitano, essenzialmente, al titolo dell'opera di cui trattasi nonché a un estratto denominato «chunk», che si presenta sotto forma di una sequenza alfanumerica e non di una captazione audio o video dell'opera.

110 A tal riguardo, è vero che non si può escludere, in generale, che l'accesso, da parte di un'autorità pubblica, a un numero limitato di dati relativi all'identità civile del titolare di un indirizzo IP che le è stato comunicato da un fornitore di servizi di comunicazione elettronica al solo scopo di identificare tale titolare nel caso in cui tale indirizzo sia stato utilizzato per attività che possono ledere i diritti d'autore o i diritti connessi, se combinato con l'analisi di informazioni, anche limitate, sul contenuto dell'opera illegittimamente messa a disposizione su Internet che le sono state trasmesse in precedenza dagli organismi degli aventi diritto, possa informare tale autorità pubblica su taluni aspetti della vita privata di tale titolare, ivi comprese informazioni sensibili, quali l'orientamento sessuale, le opinioni politiche, le convinzioni religiose, filosofiche, sociali o di altro tipo, nonché lo stato di salute, pur se tali dati godono, peraltro, di una tutela particolare nel diritto dell'Unione.

111 Tuttavia, nel caso di specie, alla luce della natura dei dati e delle informazioni limitate di cui dispone l'Hadopi, è solo in situazioni atipiche che esse potrebbero rivelare informazioni, eventualmente sensibili, su aspetti della vita privata della persona in questione che, considerati congiuntamente, potrebbero consentire a tale autorità pubblica di trarre conclusioni precise sulla vita privata di quest'ultima, ad esempio tracciandone il profilo dettagliato.

112 Ciò potrebbe verificarsi, in particolare, nel caso di una persona il cui indirizzo IP sia stato utilizzato per attività che ledono i diritti d'autore o i diritti connessi su reti tra pari (peer to peer) in modo ripetuto, o addirittura su larga scala, in relazione ad opere protette di tipo particolare che possono essere raggruppate sulla base dei termini del loro titolo idonei a rivelare informazioni, eventualmente sensibili, su aspetti della sua vita privata.

113 Ciò premesso, diversi elementi consentono di ritenere che, nel caso di specie, l'ingerenza nella vita privata di una persona, sospettata di aver svolto un'attività lesiva dei diritti d'autore o dei diritti connessi, consentita da una normativa come quella di cui trattasi nel procedimento principale non presenta necessariamente un grado di gravità elevato. Anzitutto, conformemente a siffatta normativa, l'accesso della Hadopi ai dati personali di cui trattasi è riservato a un numero limitato di agenti giurati autorizzati di tale autorità pubblica, organo che peraltro gode di uno status indipendente conformemente all'articolo L. 331-12 del CPI. Inoltre, tale accesso ha come unico scopo quello di identificare una persona sospettata di aver svolto un'attività lesiva dei diritti d'autore o dei diritti connessi qualora venga accertato che un'opera protetta è stata illegittimamente messa a disposizione a partire dal suo accesso a Internet. Infine, l'accesso della Hadopi ai dati personali in questione è strettamente limitato ai dati necessari a tal fine (v., per analogia, Corte EDU, 17 ottobre 2019, López Ribalda e a. c. Spagna, CE:ECHR:2019:1017JUD000187413, § § 126 e 127).

114 Un altro elemento idoneo a ridurre ulteriormente il grado di ingerenza, nei diritti fondamentali alla tutela della vita privata e dei dati personali, derivante da detto accesso della Hadopi, che sembra emergere dal fascicolo di cui dispone la Corte ma che incombe al giudice del rinvio verificare, riguarda il fatto che, in forza della normativa nazionale applicabile, gli agenti della Hadopi che hanno accesso ai dati e alle informazioni di cui trattasi sono tenuti ad un obbligo di riservatezza che vieta loro di divulgare tali dati e informazioni in qualsiasi forma, salvo al solo fine di adire il pubblico ministero, e di utilizzare tali dati a fini diversi dall'identificazione del titolare di un indirizzo IP sospettato di aver

commesso un'attività lesiva del diritto d'autore o di un diritto connesso al fine di imporgli una delle misure previste dalla procedura di risposta graduata (v., per analogia, Corte EDU, 17 dicembre 2009, Gardel c. Francia, CE:ECHR:2009:1217JUD001642805, § 70).

115 Pertanto, sempre che una normativa nazionale soddisfi le condizioni ricordate al punto 101 della presente sentenza, gli indirizzi IP comunicati a un'autorità pubblica quale la Hadopi non consentono di procedere al tracciamento del percorso di navigazione del loro titolare, il che tende a confermare la constatazione secondo cui l'ingerenza comportata dall'accesso di tale autorità ai dati identificativi di cui trattasi nel procedimento principale non può essere qualificata come grave.

116 In terzo luogo, occorre ricordare che, ai fini della necessaria conciliazione dei diritti e degli interessi in gioco imposta dal requisito di proporzionalità prescritto dall'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58, pur se la libertà di espressione e la riservatezza dei dati personali sono preoccupazioni primarie e gli utenti delle telecomunicazioni e dei servizi Internet devono avere la garanzia del fatto che la loro intimità e la loro libertà di espressione saranno rispettate, tali diritti fondamentali non sono assoluti. Infatti, al termine di un bilanciamento tra i diritti e gli interessi in gioco, talvolta questi ultimi devono cedere il passo dinanzi ad altri diritti fondamentali e ad imperativi di interesse generale quali la difesa dell'ordine pubblico e la prevenzione dei reati o la protezione dei diritti e delle libertà altrui. Ciò si verifica, in particolare, qualora la preponderanza accordata a dette preoccupazioni primarie sia atta a ostacolare l'efficacia di un'indagine penale, in particolare rendendo impossibile o eccessivamente difficile l'identificazione effettiva dell'autore di un reato e l'imposizione di una sanzione nei suoi confronti (v., per analogia, Corte EDU, 2 marzo 2009, K.U. c. Finlandia, CE:ECHR:2008:1202JUD000287202, § 49).

117 In tale contesto, si deve tenere debitamente conto del fatto che, come già dichiarato dalla Corte, nel caso di reati commessi online, l'accesso agli indirizzi IP può costituire l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione di detto reato (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 154).

118 Tale circostanza tende a dimostrare, come parimenti rilevato, in sostanza, dall'avvocato generale al paragrafo 59 delle sue conclusioni del 28 settembre 2023, che la conservazione di tali indirizzi e l'accesso agli stessi sono, per quanto riguarda la lotta contro reati come quelli che violano i diritti d'autore o i diritti connessi commessi online, strettamente necessari al conseguimento dell'obiettivo perseguito e soddisfano quindi il requisito di proporzionalità imposto dall'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce del considerando 11 di tale direttiva nonché dell'articolo 52, paragrafo 2, della Carta.

119 Non consentire un accesso siffatto comporterebbe peraltro, come sottolineato, in sostanza, dall'avvocato generale ai paragrafi da 78 a 80 delle sue conclusioni del 27 ottobre 2022 nonché ai paragrafi 80 e 81 delle sue conclusioni del 28 settembre 2023, un rischio reale di impunità sistemica non solo di reati che ledono i diritti d'autore o i diritti connessi, ma anche altri tipi di reati commessi online o la cui commissione o preparazione è agevolata dalle caratteristiche proprie di Internet. Orbene, l'esistenza di un rischio di questo tipo costituisce una circostanza rilevante al fine di valutare, nell'ambito di un bilanciamento dei diversi diritti e interessi in gioco, se un'ingerenza nei diritti garantiti dagli articoli 7, 8 e 11 della Carta sia una misura proporzionata rispetto all'obiettivo della lotta contro i reati.

120 È vero che l'accesso di un'autorità pubblica come la Hadopi a dati relativi all'identità civile corrispondenti all'indirizzo IP a partire dal quale è stato commesso il reato online non è necessariamente l'unico mezzo di indagine possibile per identificare la persona titolare di detto indirizzo al momento della commissione di tale reato. Un'identificazione del genere potrebbe, infatti, essere a priori parimenti possibile esaminando l'insieme delle attività online dell'interessato, in particolare analizzando le «tracce» che quest'ultimo abbia potuto lasciare sui social network, quali l'identificativo utilizzato su tali reti o le sue coordinate.

121 Tuttavia, come rilevato dall'avvocato generale al paragrafo 83 delle sue conclusioni del 28 settembre 2023, un mezzo di indagine siffatto sarebbe particolarmente invasivo in quanto potrebbe rivelare informazioni precise sulla vita privata delle persone interessate. Esso implicherebbe quindi, per tali

persone, un'ingerenza nei diritti garantiti dagli articoli 7, 8 e 11 della Carta più grave rispetto a quella derivante da una normativa come quella di cui trattasi nel procedimento principale.

122 Da quanto precede discende che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso non osta, in linea di principio, a una normativa nazionale che consente l'accesso, da parte di un'autorità pubblica incaricata della tutela dei diritti d'autore e dei diritti connessi contro violazioni di tali diritti commesse su Internet, a dati relativi all'identità civile corrispondenti a indirizzi IP in precedenza raccolti da organismi degli aventi diritto e conservati dai fornitori di servizi di comunicazione elettronica in maniera separata ed effettivamente stagna, al solo scopo di permettere a tale autorità di identificare i titolari di tali indirizzi sospettati di essere responsabili di dette violazioni e di adottare, se del caso, misure nei loro confronti. In un caso del genere, la normativa nazionale applicabile deve vietare agli agenti che dispongono di un accesso del genere, in primo luogo, di divulgare, in qualsiasi forma, informazioni sul contenuto dei file consultati da tali titolari, salvo al solo fine di adire il pubblico ministero, in secondo luogo, effettuare qualsiasi tracciamento del percorso di navigazione di tali titolari e, in terzo luogo, utilizzare tali indirizzi IP per fini diversi da quello dell'adozione delle suddette misure.

Sul requisito di un controllo da parte di un giudice o di un organismo amministrativo indipendente prima dell'accesso da parte di un'autorità pubblica a dati relativi all'identità civile corrispondenti ad un indirizzo IP

123 Si pone tuttavia la questione se l'accesso dell'autorità pubblica a dati relativi all'identità civile corrispondenti ad un indirizzo IP debba essere, inoltre, subordinato ad un controllo previo da parte di un giudice o di un organismo amministrativo indipendente.

124 A tal riguardo, al fine di garantire, in pratica, il pieno rispetto delle condizioni che gli Stati membri sono tenuti a prevedere al fine di assicurare che l'accesso sia limitato allo stretto necessario, la Corte ha dichiarato che è «essenziale» che l'accesso delle autorità nazionali competenti ai dati relativi al traffico e ai dati relativi all'ubicazione sia soggetto ad un controllo previo da parte di un giudice o di un organo amministrativo indipendente [v., in tal senso, sentenze del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15, EU:C:2016:970, punto 120; del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 189; del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 51, e del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 106].

125 Tale controllo previo richiede anzitutto che il giudice o l'organo amministrativo indipendente incaricato di effettuarlo disponga di tutte le attribuzioni e presenti tutte le garanzie necessarie per assicurare un contemperamento dei vari interessi legittimi e diritti in gioco. Per quanto riguarda, più in particolare, l'indagine penale, siffatto controllo richiede che tale giudice o tale organo sia in grado di garantire un giusto equilibrio tra, da un lato, gli interessi legittimi relativi alle esigenze dell'indagine nell'ambito della lotta alla criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso (sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 107 e giurisprudenza citata).

126 In secondo luogo, qualora tale controllo venga effettuato non da un giudice, bensì da un organo amministrativo indipendente, quest'ultimo deve godere di uno status che gli permetta di agire nell'assolvimento dei propri compiti in modo obiettivo e imparziale e deve, a tale scopo, essere al riparo da qualsiasi influenza esterna. Pertanto, il requisito di indipendenza che deve soddisfare l'autorità incaricata di esercitare il controllo previo impone che essa abbia la qualità di terzo rispetto all'autorità che chiede l'accesso ai dati, così da essere in grado di esercitare tale controllo in modo obiettivo e imparziale, al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito dell'indipendenza implica che l'autorità responsabile di tale controllo previo, da un lato, non sia coinvolta nella conduzione dell'indagine penale in questione e, dall'altro, abbia una posizione di neutralità rispetto alle parti del procedimento penale (sentenza del 5 aprile 2022 nella causa C-140/20 Commissioner of An Garda Síochána e a., EU:C:2022:258, punto 108 e giurisprudenza ivi citata).

127 In terzo luogo, il controllo indipendente richiesto ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 deve avvenire prima di qualsiasi accesso ai dati considerati, salvo in caso di urgenza debitamente giustificata, nel qual caso detto controllo deve avvenire in tempi brevi. Un controllo successivo non consentirebbe, infatti, di rispondere all'obiettivo del controllo previo, che consiste nell'impedire che sia autorizzato un accesso ai dati in questione che superi i limiti dello stretto necessario [sentenza del 5 aprile 2022, Commissioner of An Garda Síochána e a., C-140/20, EU:C:2022:258, punto 110].

128 Ciò premesso, sebbene, come risulta dalla giurisprudenza ricordata al punto 124 della presente sentenza, la Corte abbia ritenuto «essenziale» che l'accesso delle autorità nazionali competenti ai dati relativi al traffico e ai dati relativi all'ubicazione sia soggetto a un controllo previo da parte di un giudice o di un organo amministrativo indipendente, tale giurisprudenza si è sviluppata nel contesto di misure nazionali che consentivano, ai fini di un obiettivo connesso alla lotta contro le forme gravi di criminalità, un accesso generale a tutti i dati relativi al traffico e all'ubicazione conservati, a prescindere da un qualsivoglia collegamento, fosse pure indiretto, con lo scopo perseguito, e che comportavano quindi ingerenze gravi e anche «particolarmente gravi» nei diritti fondamentali considerati.

129 Per contro, allorché erano in discussione le condizioni alle quali un accesso ai dati relativi all'identità civile poteva essere giustificato alla luce dell'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 della Carta, la Corte non ha fatto alcun riferimento esplicito al requisito di un controllo previo siffatto [v., in tal senso, sentenze del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punti 59, 60 e 62; del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 157 e 158, nonché del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 34].

130 Orbene, dalla giurisprudenza della Corte relativa al principio di proporzionalità di cui l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 impone il rispetto, in particolare dalla giurisprudenza secondo la quale la possibilità per gli Stati membri di giustificare una limitazione dei diritti e degli obblighi previsti, in particolare, agli articoli 5, 6 e 9 di tale direttiva, deve essere valutata misurando la gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7, 8 e 11 della Carta che una siffatta limitazione comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito da tale limitazione sia in rapporto a tale gravità (sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto 131), discende che il grado di ingerenza nei diritti fondamentali considerati comportata dall'accesso ai dati personali di cui trattasi nonché il livello di sensibilità di questi ultimi devono parimenti influire sulle garanzie sostanziali e procedurali che devono accompagnare tale accesso, tra le quali figura il requisito di un controllo previo da parte di un giudice o di un organo amministrativo indipendente.

131 Pertanto, tenuto conto di tale principio di proporzionalità, si deve considerare che il requisito di un controllo previo da parte di un giudice o di un organo amministrativo indipendente si impone allorché, nel contesto di una normativa nazionale che prevede l'accesso di un'autorità pubblica a dati personali, tale accesso comporta il rischio di una grave ingerenza nei diritti fondamentali dell'interessato, nel senso che esso potrebbe consentire a tale autorità pubblica di trarre conclusioni precise sulla sua vita privata e, se del caso, di tracciarne il profilo dettagliato.

132 Al contrario, tale requisito di un controllo previo non è inteso applicarsi quando non può essere qualificata come grave l'ingerenza nei diritti fondamentali interessati comportata dall'accesso di un'autorità pubblica a dati personali.

133 Tale ipotesi ricorre nel caso dell'accesso a dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica al solo scopo di identificare l'utente considerato e senza che tali dati possano essere associati a informazioni relative alle comunicazioni effettuate, poiché, secondo la giurisprudenza della Corte, l'ingerenza comportata da un trattamento siffatto di detti dati non può, in linea di principio, essere qualificata come grave (v., in tal senso, sentenza del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 157 e 158).

134 Ne consegue che, nel caso in cui è istituito un dispositivo di conservazione del tipo descritto ai punti da 86 a 89 della presente sentenza, l'accesso dell'autorità pubblica ai dati relativi all'identità civile

corrispondenti agli indirizzi IP così conservati non è, in linea di principio, subordinato al requisito di un controllo previo da parte di un giudice o di un organo amministrativo indipendente.

135 Ciò premesso, come già rilevato ai punti 110 e 111 della presente sentenza, non si può escludere che, in situazioni atipiche, i dati e le informazioni limitati messi a disposizione di un'autorità pubblica nell'ambito di un procedimento come quello della risposta graduata di cui trattasi nel procedimento principale possano rivelare informazioni, se del caso sensibili, su aspetti della vita privata della persona di cui trattasi, informazioni che, considerate congiuntamente, potrebbero consentire a tale autorità pubblica di trarre conclusioni precise sulla vita privata di quest'ultimo e, se del caso, di tracciarne il profilo dettagliato.

136 Come risulta dal punto 112 della presente sentenza, un siffatto rischio per la vita privata può presentarsi, in particolare, quando una persona compie attività che violano i diritti d'autore o i diritti connessi su reti tra pari (peer to peer) in modo ripetuto, o addirittura su larga scala, collegate a opere protette di tipi particolari che possono essere raggruppate sulla base dei termini del loro titolo, rivelanti informazioni, eventualmente sensibili, sulla sua vita privata.

137 Pertanto, nel caso di specie, nell'ambito del procedimento amministrativo di risposta graduata, un titolare di un indirizzo IP può essere particolarmente esposto a un siffatto rischio per la sua vita privata qualora tale procedimento raggiunga la fase in cui la Hadopi è chiamata a decidere di adire o meno il pubblico ministero ai fini dell'esercizio dell'azione penale nei confronti di tale titolare per fatti che possono costituire la contravvenzione di negligenza grave o per il reato (délit) di contraffazione.

138 Tale adizione presuppone, infatti, che detto titolare sia già stato oggetto di due raccomandazioni e di una lettera di notifica che lo informi del fatto che le sue attività possono essere perseguite penalmente, misure che implicano che, ogni volta, la Hadopi abbia avuto accesso a dati relativi all'identità civile di detto titolare, il cui indirizzo IP è stato utilizzato per attività lesive dei diritti d'autore o dei diritti connessi, nonché ad un file relativo a tale opera contenente, essenzialmente, il suo titolo.

139 Ebbene, non si può escludere che, considerati congiuntamente e man mano che si svolge il procedimento amministrativo di risposta graduata, i dati così forniti nelle diverse fasi di tale procedimento possano rivelare informazioni concordanti e, eventualmente, sensibili su aspetti della vita privata dell'interessato che consentano, se del caso, di tracciarne il profilo.

140 Pertanto, l'intensità della violazione del diritto al rispetto della vita privata può aumentare man mano che la procedura di risposta graduata, che opera secondo un processo sequenziale, percorra le diverse fasi che la compongono.

141 Nel caso di specie, l'accesso della Hadopi al complesso dei dati relativi all'interessato cumulati nel corso delle diverse fasi di tale procedura può, per il fatto di mettere in relazione tali dati, consentire di trarre conclusioni precise sulla vita di quest'ultimo. Pertanto, nell'ambito di un procedimento come quello della risposta graduata di cui trattasi nel procedimento principale, la normativa nazionale deve altresì prevedere, in una qualche fase di detto procedimento, un previo controllo da parte di un giudice o di un organo amministrativo indipendente, che soddisfi le condizioni ricordate ai punti da 125 a 127 della presente sentenza, al fine di escludere rischi di ingerenze sproporzionate nei diritti fondamentali alla tutela della vita privata e dei dati personali dell'interessato. Ciò significa, in pratica, che un controllo siffatto deve avvenire prima che la Hadopi possa mettere in relazione i dati relativi all'identità civile di una persona, che è già oggetto di due raccomandazioni corrispondenti a un indirizzo IP, ottenuti presso un fornitore di servizi di comunicazione elettronica, e il file relativo all'opera messa a disposizione su Internet per essere scaricata da altre persone. Pertanto, detto controllo deve avvenire prima dell'eventuale invio della lettera di notifica di cui all'articolo R-331-40 del CPI, che constata che tale persona ha commesso fatti che possono costituire il reato di negligenza grave. È solo a seguito di un controllo previo di questo tipo da parte di un giudice o di un organismo amministrativo indipendente e della loro autorizzazione che l'Hadopi potrà inviare siffatta lettera e successivamente, se del caso, adire il pubblico ministero ai fini della repressione di tale reato.

142 Occorre consentire alla Hadopi di individuare i casi in cui il titolare dell'indirizzo IP interessato raggiunge questa terza fase di una procedura di risposta graduata del genere. Pertanto, tale procedura deve essere organizzata e strutturata in modo tale che i dati relativi all'identità civile di una persona

corrispondenti a indirizzi IP precedentemente raccolti su Internet, riuniti presso fornitori di servizi di comunicazione elettronica, non possano essere automaticamente messi in relazione, dalle persone incaricate dell'esame dei fatti all'interno della Hadopi, con i file contenenti elementi che consentano di conoscere i titoli delle opere protette che hanno giustificato tale raccolta.

143 Quindi, tale messa in relazione ai fini della suddetta terza fase della risposta graduata deve essere sospesa allorché la raccolta di detti dati relativi all'identità civile, che corrispondono ad un caso di seconda possibile reiterazione di un'attività lesiva dei diritti d'autore o dei diritti connessi, comporta la necessità di un previo controllo da parte di un giudice o di un organo amministrativo indipendente descritto al punto 141 della presente sentenza.

144 Peraltro, la configurazione del requisito del controllo previo esposta ai punti da 141 a 143 della presente sentenza, per il fatto di essere limitata alla terza fase di detta procedura di risposta graduata e di non applicarsi alle fasi precedenti di quest'ultima, consente altresì di prendere in considerazione l'argomento secondo cui occorre salvaguardare la praticabilità di tale procedura, che è caratterizzata, soprattutto nelle sue fasi precedenti all'eventuale invio della lettera di notifica e, se del caso, all'adizione del pubblico ministero, dalla ingente quantità di domande di accesso dell'autorità pubblica derivante dal numero altrettanto ingente di verbali di cui tale autorità è investita da parte degli organismi degli aventi diritto.

145 Per quanto riguarda, inoltre, l'oggetto del controllo previo di cui ai punti da 141 a 143 della presente sentenza, dalla giurisprudenza ricordata ai punti 95 e 96 della presente sentenza risulta che, nel caso in cui la persona interessata sia sospettata di aver commesso il reato di «negligenza grave» definito all'articolo R. 335-5 del CPI, rientrante nei reati in generale, il giudice o l'organismo amministrativo indipendente incaricato di tale controllo deve negare l'accesso qualora quest'ultimo consenta all'autorità pubblica che l'ha richiesto di trarre conclusioni precise sulla vita privata di detta persona.

146 Per contro, anche un accesso che consenta di trarre siffatte conclusioni precise dovrebbe essere autorizzato nel caso in cui gli elementi portati a conoscenza di tale giudice o organismo amministrativo indipendente consentano di sospettare che la persona interessata abbia commesso il reato (délit) di contraffazione di cui all'articolo L. 335-2 del CPI o all'articolo L. 335-4 di tale codice, dato che uno Stato membro può ritenere che un reato di questo tipo, in quanto lesivo di un interesse fondamentale della società, rientri nelle forme gravi di criminalità.

147 Infine, per quanto riguarda le modalità di tale controllo previo, il governo francese ritiene che, alla luce delle caratteristiche particolari dell'accesso da parte dell'Hadopi ai dati di cui trattasi, in particolare dell'ingente numero di tali accessi, sia appropriato che un controllo previo, se necessario, sia interamente automatizzato. Un controllo del genere, che ha carattere puramente oggettivo, mirerebbe, infatti, essenzialmente a verificare che il verbale di adizione della Hadopi contenga tutte le informazioni e i dati richiesti senza che tale autorità sia chiamata a valutarli.

148 Tuttavia, un controllo previo non può in nessun caso essere completamente automatizzato poiché, come risulta dalla giurisprudenza ricordata al punto 125 della presente sentenza, trattandosi di un'indagine penale, un controllo del genere richiede, in ogni caso, che il giudice o l'organismo amministrativo indipendente considerato sia in grado di garantire un giusto equilibrio tra, da un lato, i legittimi interessi connessi alle esigenze dell'indagine nell'ambito della lotta contro la criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono oggetto dell'accesso.

149 Un bilanciamento siffatto dei diversi interessi legittimi e dei diritti di cui trattasi richiede, infatti, l'intervento di una persona fisica, e ciò è tanto più necessario in quanto l'automaticità e la grande scala del trattamento di dati di cui trattasi comportano rischi per la vita privata.

150 Inoltre, un controllo interamente automatizzato non è, in linea di principio, idoneo a garantire che l'accesso non ecceda i limiti dello stretto necessario e che le persone i cui dati personali sono interessati dispongano di garanzie effettive contro i rischi di abuso nonché contro qualsiasi accesso a tali dati e qualsiasi uso illecito degli stessi.

151 Pertanto, anche se controlli automatizzati possono consentire di verificare talune delle informazioni contenute nei verbali degli organismi degli aventi diritto, tali controlli devono, in ogni caso, andare di pari passo con controlli da parte di persone fisiche che rispondano pienamente ai requisiti ricordati ai punti da 125 a 127 della presente sentenza.

Sui requisiti, attinenti alle condizioni sostanziali e procedurali e altresì alle garanzie contro i rischi di abuso nonché contro qualsiasi accesso e uso illeciti di tali dati, che si impongono all'accesso da parte di un'autorità pubblica a dati relativi all'identità civile corrispondenti a un indirizzo IP

152 Dalla giurisprudenza della Corte risulta che l'accesso a dati personali può essere conforme al requisito di proporzionalità imposto dall'articolo 15, paragrafo 1, della direttiva 2002/58 solo se la misura legislativa che lo autorizza prevede, mediante norme chiare e precise, che detto accesso sia subordinato al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongano di garanzie effettive contro i rischi di accesso e di uso abusivi o illeciti di tali dati [v., in tal senso, sentenze del 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punti 132 e 173, nonché del 2 marzo 2021, Prokuratuur (Condizioni di accesso ai dati relativi alle comunicazioni elettroniche), C-746/18, EU:C:2021:152, punto 49 e giurisprudenza ivi citata].

153 Come sottolineato dalla Corte, la necessità di tali garanzie è ancora più importante quando i dati personali sono soggetti a trattamento automatizzato (sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, punto 176 e giurisprudenza ivi citata).

154 Al riguardo, in risposta ad un quesito posto dalla Corte in vista dell'udienza del 5 luglio 2022, il governo francese ha confermato che, come peraltro indicato dall'articolo L. 331-29 del CPI, l'accesso da parte della Hadopi ai dati relativi all'identità civile nell'ambito della procedura di risposta graduata deriva da un trattamento di dati essenzialmente automatizzato che si spiega con l'ingente numero delle contraffazioni constatate sulle reti tra pari (peer to peer) dagli organismi di aventi diritto, constatazioni che sono trasmesse all'Hadopi sotto forma di verbali.

155 Dal fascicolo di cui dispone la Corte risulta in particolare che, in occasione di tale trattamento di dati, gli agenti della Hadopi verificano, in modo essenzialmente automatizzato e senza valutazione dei fatti di cui trattasi in quanto tali, se i verbali di cui essa è investita contengano tutte le informazioni e i dati menzionati al punto 1º dell'allegato al decreto n. 2010-236, in particolare i fatti di messa a disposizione illegittima su Internet considerati e gli indirizzi IP utilizzati a tal fine. Ebbene, trattamenti del genere devono andare di pari passo con controlli da parte di persone fisiche.

156 Poiché un siffatto trattamento automatizzato può comportare un certo numero di casi di falso positivo nonché, soprattutto, il rischio che un numero di dati personali potenzialmente molto elevato sia sviato da terzi a fini abusivi o illeciti, occorre che, in forza di una misura legislativa, il sistema di trattamento dei dati utilizzato da un'autorità pubblica sia sottoposto, a intervalli regolari, ad un controllo da parte di un organismo indipendente avente la qualità di terzo rispetto a tale autorità, al fine di verificare l'integrità del sistema, comprese le garanzie effettive contro i rischi di abuso nonché contro qualsiasi accesso a tali dati e qualsiasi uso illecito di questi ultimi che tale sistema deve assicurare, nonché la sua efficacia e affidabilità nel rilevare le violazioni che possono essere qualificate, in caso di reiterazione, come negligenza grave o contraffazione.

157 Occorre, infine, aggiungere che un trattamento di dati personali effettuato da un'autorità pubblica, come quello cui procede l'Hadopi nell'ambito della procedura di risposta graduata, deve rispettare le norme specifiche di protezione di tali dati previste dalla direttiva 2016/680, il cui scopo è, ai sensi del suo articolo 1, stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

158 Nel caso di specie, infatti, anche se, in forza del diritto nazionale applicabile, essa non dispone di poteri decisionali propri, l'Hadopi, quando tratta nell'ambito del procedimento di risposta graduata i dati personali e adotta misure quali una raccomandazione o l'informazione alla persona interessata secondo la quale i fatti di cui trattasi sono perseguibili penalmente, deve essere qualificata come «autorità pubblica», ai sensi dell'articolo 3 della direttiva 2016/680, coinvolta nella prevenzione e

nell'accertamento dei reati, vale a dire la contravvenzione per negligenza grave o il reato (délit) di contraffazione, e rientra quindi nell'ambito di applicazione di tale direttiva conformemente al suo articolo 1.

159 A tal riguardo, il governo francese ha indicato, in risposta ad un quesito posto dalla Corte in vista dell'udienza del 5 luglio 2022, che, poiché le misure adottate dall'Hadopi nell'ambito della messa in atto del procedimento di risposta graduata «hanno carattere prepenale direttamente connesso al procedimento giudiziario», il sistema di gestione delle misure per la protezione delle opere su Internet, attuato dalla Hadopi, è soggetto, come risulta dalla giurisprudenza del giudice del rinvio, alle disposizioni di diritto nazionale dirette a trasporre la direttiva 2016/680.

160 Per contro, un trattamento di dati siffatto da parte dell'Hadopi non rientra nell'ambito di applicazione del RGPD. Infatti, l'articolo 2, paragrafo 2, lettera d), del RGPD dispone che tale regolamento non si applica ai trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

161 Come rilevato dall'avvocato generale al paragrafo 104 delle sue conclusioni del 27 ottobre 2022, poiché il rispetto della direttiva 2016/680 si impone quindi alla Hadopi nell'ambito della procedura di risposta graduata, le persone coinvolte in una siffatta procedura devono beneficiare di un insieme di garanzie sostanziali e procedurali comprendenti il diritto di accesso, di rettifica e di cancellazione dei dati personali trattati dall'Hadopi nonché la possibilità di presentare un reclamo presso un'autorità di controllo indipendente, seguito, se del caso, da un ricorso giurisdizionale esperito alle condizioni di diritto comune.

162 In tale contesto, dalla normativa nazionale di cui trattasi nel procedimento principale risulta che, nell'ambito del procedimento di risposta graduata, più precisamente al momento dell'invio della seconda raccomandazione e al momento della successiva notifica che i fatti accertati possono essere qualificati come reato, il destinatario di tali comunicazioni gode di talune garanzie procedurali quali il diritto di presentare osservazioni, il diritto di ottenere precisazioni sulla violazione contestatagli nonché, per quanto riguarda detta notifica, il diritto di chiedere un'audizione e di farsi assistere da un difensore.

163 In ogni caso, spetta al giudice del rinvio verificare se tale normativa nazionale preveda tutte le garanzie sostanziali e procedurali prescritte dalla direttiva 2016/680.

164 Alla luce di tutte le considerazioni che precedono, occorre rispondere alle tre questioni pregiudiziali dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso non osta a una normativa nazionale che autorizza l'autorità pubblica incaricata della protezione dei diritti d'autore e dei diritti connessi contro le violazioni di tali diritti commesse su Internet ad accedere ai dati, conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico, relativi all'identità civile corrispondenti a indirizzi IP precedentemente raccolti da organismi degli aventi diritto, affinché tale autorità possa identificare i titolari di tali indirizzi, utilizzati per attività che possono costituire violazioni del genere, e possa adottare, eventualmente, misure nei loro confronti, purché, in forza di tale normativa,

– tali dati siano conservati in condizioni e secondo modalità tecniche che garantiscano che sia escluso che tale conservazione possa consentire di trarre conclusioni precise sulla vita privata di detti titolari – ad esempio tracciandone il profilo dettagliato – ciò può essere conseguito, in particolare, imponendo ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione delle diverse categorie di dati personali, quali i dati relativi all'identità civile, gli indirizzi IP nonché i dati relativi al traffico e i dati relativi all'ubicazione, che garantisca una separazione effettivamente stagna di tali diverse categorie di dati tale da impedire, nella fase della conservazione, qualsiasi utilizzo combinato di dette diverse categorie di dati, e per un periodo non superiore allo stretto necessario,

– l'accesso della suddetta autorità pubblica a tali dati conservati in maniera separata ed effettivamente stagna serva esclusivamente a identificare la persona sospettata di aver commesso

un reato e sia accompagnato dalle garanzie necessarie per escludere che, salvo in situazioni atipiche, tale accesso possa consentire di trarre conclusioni precise sulla vita privata dei titolari degli indirizzi IP – ad esempio tracciandone il profilo dettagliato – ciò che implica, in particolare, che sia vietato ai funzionari di tale autorità, autorizzati ad avere un siffatto accesso, di divulgare, in qualsiasi forma, informazioni sul contenuto dei file consultati da detti titolari – salvo al solo fine di adire il pubblico ministero –; procedere a un tracciamento del percorso di navigazione di tali titolari e, più in generale, utilizzare tali indirizzi IP per uno scopo diverso da quello di identificare i loro titolari ai fini dell'adozione di eventuali misure contro questi ultimi,

– la possibilità, per le persone incaricate dell'esame dei fatti all'interno di detta autorità pubblica, di mettere in relazione tali dati con i file contenenti elementi che consentono di conoscere il titolo di opere protette la cui messa a disposizione in Internet ha giustificato la raccolta degli indirizzi IP da parte di organismi degli aventi diritto, sia subordinata, nelle ipotesi di nuova reiterazione di un'attività lesiva dei diritti d'autore o dei diritti connessi da parte di uno stesso soggetto, a un controllo, da parte di un giudice o di un organismo amministrativo indipendente, che non può essere interamente automatizzato e deve avvenire prima di tale messa in relazione, in quanto tale messa in relazione può, in tali ipotesi, consentire di trarre precise conclusioni sulla vita privata di detto soggetto, il cui indirizzo IP sia stato utilizzato per attività che possono ledere i diritti d'autore o i diritti connessi,

– il sistema di trattamento dei dati utilizzato dall'autorità pubblica sia sottoposto, a intervalli regolari, ad un controllo da parte di un organismo indipendente, avente la qualità di terzo rispetto alla suddetta autorità pubblica, al fine di verificare l'integrità del sistema, comprese le garanzie effettive contro i rischi di accesso e uso impropri o illeciti di tali dati, nonché la sua efficacia e affidabilità nel rilevare eventuali violazioni.

Sulle spese

165 Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (seduta plenaria) dichiara:

L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8, 11 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea.

deve essere interpretato nel senso che:

esso non osta a una normativa nazionale che autorizza l'autorità pubblica incaricata della protezione dei diritti d'autore e dei diritti connessi contro le violazioni di tali diritti commesse su Internet ad accedere ai dati, conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico, relativi all'identità civile corrispondenti a indirizzi IP precedentemente raccolti da organismi degli aventi diritto, affinché tale autorità possa identificare i titolari di tali indirizzi, utilizzati per attività che possono costituire violazioni del genere, e possa adottare, eventualmente, misure nei loro confronti, purché, in forza di tale normativa,

– **tali dati siano conservati in condizioni e secondo modalità tecniche che garantiscano che sia escluso che tale conservazione possa consentire di trarre conclusioni precise sulla vita privata di detti titolari – ad esempio tracciandone il profilo dettagliato – ciò può essere conseguito, in particolare, imponendo ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione delle diverse categorie di dati personali, quali i dati relativi all'identità civile, gli indirizzi IP nonché i dati relativi al traffico e i dati relativi**

all'ubicazione, che garantisca una separazione effettivamente stagna di tali diverse categorie di dati tale da impedire, nella fase della conservazione, qualsiasi utilizzo combinato di dette diverse categorie di dati, e per un periodo non superiore allo stretto necessario,

– **l'accesso della suddetta autorità pubblica a tali dati conservati in maniera separata ed effettivamente stagna serva esclusivamente a identificare la persona sospettata di aver commesso un reato e sia accompagnato dalle garanzie necessarie per escludere che, salvo in situazioni atipiche, tale accesso possa consentire di trarre conclusioni precise sulla vita privata dei titolari degli indirizzi IP – ad esempio tracciandone il profilo dettagliato – ciò che implica, in particolare, che sia vietato ai funzionari di tale autorità, autorizzati ad avere un siffatto accesso, di divulgare, in qualsiasi forma, informazioni sul contenuto dei file consultati da detti titolari – salvo al solo fine di adire il pubblico ministero –; procedere a un tracciamento del percorso di navigazione di tali titolari e, più in generale, utilizzare tali indirizzi IP per uno scopo diverso da quello di identificare i loro titolari ai fini dell'adozione di eventuali misure contro questi ultimi,**

– **la possibilità, per le persone incaricate dell'esame dei fatti all'interno di detta autorità pubblica, di mettere in relazione tali dati con i file contenenti elementi che consentono di conoscere il titolo di opere protette la cui messa a disposizione in Internet ha giustificato la raccolta degli indirizzi IP da parte di organismi degli aventi diritto, sia subordinata, nelle ipotesi di nuova reiterazione di un'attività lesiva dei diritti d'autore o dei diritti connessi da parte di uno stesso soggetto, a un controllo, da parte di un giudice o di un organismo amministrativo indipendente, che non può essere interamente automatizzato e deve avvenire prima di tale messa in relazione, in quanto tale messa in relazione può, in tali ipotesi, consentire di trarre precise conclusioni sulla vita privata di detto soggetto, il cui indirizzo IP sia stato utilizzato per attività che possono ledere i diritti d'autore o i diritti connessi,**

– **il sistema di trattamento dei dati utilizzato dall'autorità pubblica sia sottoposto, a intervalli regolari, ad un controllo da parte di un organismo indipendente, avente la qualità di terzo rispetto alla suddetta autorità pubblica, al fine di verificare l'integrità del sistema, comprese le garanzie effettive contro i rischi di accesso e uso impropri o illeciti di tali dati, nonché la sua efficacia e affidabilità nel rilevare eventuali violazioni.**

Firme

---

* Lingua processuale: il francese.